A Comprehensive Survey on Cooperative Relaying and Jamming Strategies for Physical Layer Security

Preprint · July 2018

CITATIONS
0

READS
1,370

4 authors:

Furqan Jameel
Aalto University
59 PUBLICATIONS **286** CITATIONS
SEE PROFILE

Shurjeel Wyne
COMSATS University Islamabad
52 PUBLICATIONS **1,123** CITATIONS
SEE PROFILE

Georges Kaddoum
École de Technologie Supérieure
222 PUBLICATIONS **2,997** CITATIONS
SEE PROFILE

Trung Q. Duong
Queen's University Belfast
395 PUBLICATIONS **7,956** CITATIONS
SEE PROFILE

A Comprehensive Survey on Cooperative Relaying and Jamming Strategies for Physical Layer Security

Furqan Jameel, Shurjeel Wyne, Georges Kaddoum, Trung Q. Duong

***Abstract*—Physical layer security (PLS) has been extensively explored as an alternative to conventional cryptographic schemes for securing wireless links. Of late, the research community is actively working towards exploiting cooperative communication techniques to further improve the security. Many studies are showing that the cooperation between the legitimate nodes of a network can significantly enhance their secret communications, relative to the non-cooperative case. Motivated by the importance of this class of PLS systems, this paper provides a comprehensive survey of the recent works on cooperative relaying and jamming techniques for securing wireless transmissions against eavesdropping nodes which attempt to intercept the transmissions. First, it provides a in-depth overview of various secure relaying strategies and schemes. Next, a review of recently proposed solutions for cooperative jamming techniques has been provided with an emphasis on power allocation and beamforming techniques. Then, the latest developments in hybrid techniques, that use both cooperative relaying and jamming, are elaborated. Finally, several key challenges in the domain of cooperative security are presented along with an extensive discussion on the applications of cooperative security in key enablers for 5G communications, such as non-orthogonal multiple access (NOMA), device-to-device (D2D) communications, and massive multiple-input multiple-output (MIMO) systems.**

***Index Terms*—Physical layer security (PLS), 5G communications, Relaying protocols, Jamming techniques**

I. Introduction

The broadcast nature of wireless transmissions allows any receiver, within its coverage region, to capture the transmitted signal. This makes information security a major concern in the design of wireless networks. Recent advances in wireless technologies, such as the long-term evolution for cellular networks and Wi-Fi systems, have caused an exponential growth in the number of connected devices [1] which in turn entails the risk of increasing security threats, like data hacking and eavesdropping. Through cryptographic approaches, data security has been traditionally addressed at the higher layers of the open system's interconnected model, whereby the plain text message is encrypted by using powerful algorithms that assume limited computational capacity of potential eavesdroppers [2]. However, due to recent enhancements in computational power of devices and optimization strategies for breaking encryption codes, there is a need for better security strategies to protect information from unauthorized devices. Another drawback of the conventional cryptographic schemes is the requirement for key management to exchange the secret key between legitimate entities. Key sharing requires a trusted entity which cannot always be ensured in distributed wireless networks, like wireless sensor networks and wireless adhoc networks. On the other hand, the lower layers (physical and data link layers) are oblivious of any security considerations. Considering the recent challenges, security must be considered on physical layer to increase the robustness of existing schemes.

Physical layer security (PLS) was pioneered by Shannon and further discussed by Wyner [3], [4], [5], and thereafter has been identified as an appealing strategy to cope with the ever-increasing secrecy demands from the information theoretic perspective. In the recent years, PLS has been investigated both as an alternative and as a complementary approach to conventional cryptographic methods [6]. The PLS schemes exploit the random fading in wireless propagation channels to secure the communication link, while assuming no restrictions on the eavesdropper's computational power [4]. Consisting in a pair of legitimate transmitter and receiver (also known as Alice and Bob), a PLS's general wiretap model tries to communicate with the presence of an eavesdropper (also called Eve), as shown in Figure 1. Alice encodes a message w^k into a codeword $X^n = (X(1), X(2), ...X(n))$ and transmits to Bob; where k and n denote the number of message bits and codeword symbols, respectively. The signal received at Bob can be written as $Y^n = (Y(1), Y(2), ...Y(n))$ whereas the signal received at the eavesdropper is given as $Z^n = (Z(1), Z(2), ...Z(n))$. It is simply assumed that both Bob and Eve experience quasi-static fading. The signal $Y(i)$ received by Bob is written as

$$Y(i) = G_m(i)X(i) + \aleph_m(i). \tag{1}$$

Similarly, the signal received at Eve can be determined as

$$Z(i) = G_e(i)X(i) + \aleph_e(i), \tag{2}$$

where $i = 1, 2, ...n$ is the length of the signal, $\aleph_m$ and $\aleph_e$ represents the Gaussian Noise with zero mean and variance N_m and N_e for main and wiretap links, respectively. Moreover, G_m and G_e denote the channel amplitude gains of main and wiretap channels, respectively.

Wyner's contribution is mainly introducing the concept of a wiretap channel for discrete memoryless channel. Subsequently, research efforts were directed towards exploring PLS in Gaussian channels [7], [8] and then fading channels [9], [10]. Although recent studies were more focused towards ensuring perfect secrecy, more efforts were directed towards weak secrecy, by further investigating the impact of fading of secrecy performance [11], [12]. To incorporate different kinds of eavesdroppers, extensive studies for passive and active eavesdropping scenarios were provided [13]. A radio eavesdropper, also called passive eavesdropper, is capable of detecting and intercepting the main transmission without bringing any changes in the network. Also, they cannot make any modifications at the intended receiver's obtained message. Resultantly, this type of attack is difficult to detect. On the contrary, an active eavesdropper can intercept and monitor a

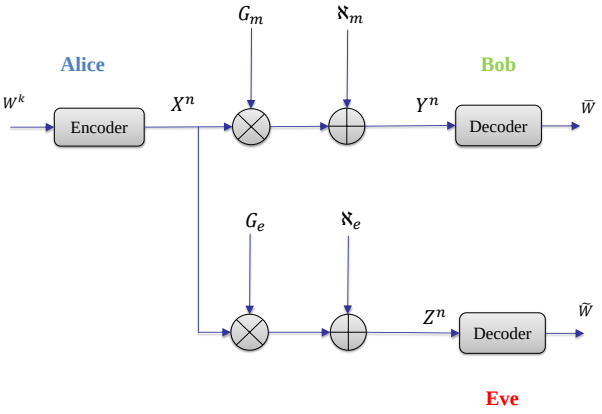


Fig. 1: Fundamental wiretap scenario.

transmission and have the capability to bring modifications in the main channel [14]. The major aim of this type of attack is to degrade the received signal at the intended receiver, causing more decoding errors. In case of multiple adversaries, eavesdroppers can work independently (non-collusion) or cooperatively (collusion). Non-colluding eavesdroppers are mutually independent and do not share received information to cooperatively decode the confidential message [15], [16], [17], whereas, colluding eavesdroppers try to intercept the communication and mutually share the information, such as received signal-to-noise ratio (SNR), to decode the message [18], [19]. A wireless link from a source to eavesdroppers can then be considered as a single-input multiple-output (SIMO) link [20]. Despite the continued research interest in PLS schemes, as shown in Table I, many open problems remain. For instance, practical coding techniques for PLS and their performance metrics are mostly unknown [21].

A. Related Surveys

The cooperative relaying and jamming strategies in the PLS has been plentifully discussed in the literature. However, very few comprehensive surveys discuss all aspects, requirements and challenges of the cooperative security. For instance, in [30], the attacks in cognitive radio networks are categorized into learning attack, primary user emulation, data falsification, jamming attack, objective function attack and eavesdropping. The authors also characterize the secrecy capacity for cognitive radio networks, in the presence of multiple eavesdroppers. In [31], Yang *et al*. have provided a detailed survey on PLS and state-of-the-art in 5G networks. The authors analyzed the three most dominant 5G technologies; heterogeneous networks (a multi-tier system having multiple devices with different characteristics), massive multiple-input multiple-output (MIMO) and millimeter-wave (mmWave) technologies. The authors also highlight various opportunities and challenges for each of these aforementioned technologies. In [32], the authors investigated code design for security and reviewed the state-of-the-art of polar codes, low-density parity-check (LDPC) codes, and lattice codes. In addition, they also surveyed the recent advances in PLS techniques for massive MIMO, mmWave, Heterogeneous networks and full-duplex technology. In [33], the literature review on PLS techniques was presented from the perspective of imperfect channel estimation. More specifically, the authors presented a high-level overview of the advancements in PLS for various wireless networks and discussed approaches for the design of secret key exchange and signal processing techniques for secrecy enchantment under imperfect channel estimation. In [34], Trappe *et al*. focused on different challenges of PLS. They highlighted various practical aspects of PLS that are require reserch attention, and discussed various benefits attached to these solutions. Mukherjee *et al*. in [35] studied PLS in detail for different multi-user conditions and presented various protocols for secret key exchange as well as approaches for code-design for information theoretic secrecy. The authors also provided future research directions for practical realization of PLS. An overview of physical layer based secure communication strategies was provided in [36]. After reviewing several information-theoretic studies, the authors asserted that despite numerous idealized assumptions in the PLS literature, game-theoretic strategies and multi-antenna transmission techniques can potentially help realize the vision of unbreakable and keyless security in wireless links. A brief survey of recent literature for jamming techniques was presented in [37]. The authors provided a description of various jamming techniques and highlighted their associated advantages and disadvantages.

B. Motivation and Contribution

While these surveys are the closest to the work presented in this paper, it is noteworthy to mention that the material our document presents is a continuation, as well as an update, of the recent achievements in the field related to the emphasis on the PLS implementation, with the cooperation of helping nodes. Specifically, we discuss recent developments in secure communications through cooperative relaying and cooperative jamming strategies. Thus, our work's intention is not limited to different cooperative PLS schemes and jamming techniques; rather, we aim to provide a taxonomy of the different proposed approaches in this area. The main contributions of this work can be summarized as follows:

1) Providing a brief overview of cooperative relaying and jamming techniques.
2) Developing a literature taxonomy of cooperative relaying and jamming, and hybrid techniques.
3) Discussing several open problems in secure cooperative relaying and jamming.
4) Presenting applications of cooperative security for 5G technologies including energy harvesting networks, relay-aided device-to-device communications and massive MIMO systems.

Finally, for clarity, a taxonomy of the cooperative relaying and jamming schemes surveyed in this work is provided in Figure 2.

C. Paper Organization

The remainder of the paper is organized as follows. Section II discusses some fundamentals of cooperative relaying for

TABLE I: Recent research trends in PLS.

Security Issue	Reference	Network Type	Solution
Authentication	[22], [23]	Wireless network	Fingerprinting
	[24]	Wireless Body Area Networks	Wireless channel exploitation
	[25]	Mobile network	Time varying carrier frequency offset
	[26]	Cognitive radio networks	Authentic tag generation by one-way hash chain
Key Agreement	[27]	Mobile networks	Deep fade detection for randomness extraction; Light-weight information reconciliation
Secrecy capacity enhancement	[28], [29]	Cooperative wireless network	Optimization
	[30]	Cognitive radio networks	Cooperative jamming
	[29]	Cellular networks	Stochastic geometry and random matrix theory

PLS. Section III provides an exhaustive discussion on secure relaying techniques. In Section IV, various cooperative jamming schemes are reviewed. Section V summarizes various hybrid cooperative strategies while Section VI discusses the application of cooperative PLS in future 5G technologies. Finally, Section VII provides some concluding remarks. A list of acronyms used in this work is provided in Table II.

II. Fundamentals of Physical Layer Security

This section reviews some key concepts, necessary for understanding information theoretic security in cooperative networks.

A. Performance Metrics

For the readers' comprehension, some of the secrecy performance metrics have been highlighted.

1) Secrecy Rate: It is the information transmission rate for the secret message, represented as

$$R_s = \frac{H(W)}{n} \tag{3}$$

where $H(.)$ is the entropy of the confidential message.

2) Equivocation Rate: It is a measure of the eavesdropper uncertainty about the confidential message W, given that Z^n has been received at the eavesdropper. It can be expressed as

$$R_{eq} = \frac{H(W|Z^n)}{n} \tag{4}$$

3) Perfect Secrecy: In case of physical layer security, the perfect secrecy is assumed to be achieved if specific conditions are achieved for (M, n) codes:

$$R_s = R_{eq} \tag{5}$$

The amount of information leakage can be represented as

$$R_s - R_{eq} = \frac{I(W; Z^n)}{n}, \tag{6}$$

where $I(.)$ represents the mutual information function. It can be noted that $n \to \infty$, $R_s - R_{eq} = 0$ and hence, no information is leaked to the eavesdropper.

4) Secrecy Capacity: The secrecy capacity C_{sec} for a wireless channel can be defined as the maximum achievable secrecy rate R_s [10]. Mathematically, it can be written as

$$C_{sec} = sup_{P_e<\varepsilon} R_s, \tag{7}$$

where $P_e = \Pr(\bar{W} \neq W)$ is the probability of error, which is a measure of the reliability of information at Bob, $\bar{W}$ is the decoded message at Bob and $\varepsilon > 0$. The secrecy capacity can alternatively be written as [36]

$$C_{sec} = \max_{p(u,x)} I(U; Y^n) - I(U; Z^n). \tag{8}$$

where U is an auxiliary random variable, which creates two virtual channels from $U \to Y$ and $U \to Z$ according to the concept of channel prefixing [38]. Then determining the secrecy capacity is virtually the same as finding the joint probability distribution of X and U $p(u, x)$ that maximizes the difference between the mutual information of the main and the wiretap links. Then by invoking the Shannon capacity theorem (8) can be rewritten as

$$C_{sec} = [C_s - C_e]^+, \tag{9}$$

where the notation $[x]^+$ represents $\max\{0, x\}$, and C_s and C_e are the channel capacities of the main and the wiretap link, respectively. The main condition here is that $C_s > C_e$, which emphasizes the fact that the main channel must be better than the wiretap channel, irrespective of the eavesdropper's computational power. This is another motivation to exploit cooperative communications to provide this much-desired advantage of the main channel.

5) Secrecy Outage Probability: The outage probability of secrecy capacity, also called secrecy outage probability (SOP), is the likelihood of achieving a non-negative target secrecy rate. In the presence of an eavesdropper in the fading channel, SOP is one of the most commonly used secrecy performance metrics. It can be formulated as [39]

$$P_{out} = \Pr(C_{sec} < R_s). \tag{10}$$

6) Intercept Probability: It is the probability that the secrecy capacity C_{sec} falls below 0 [40], [41], [42], which is given as

$$P_{int} = \Pr(C_{sec} < 0). \tag{11}$$

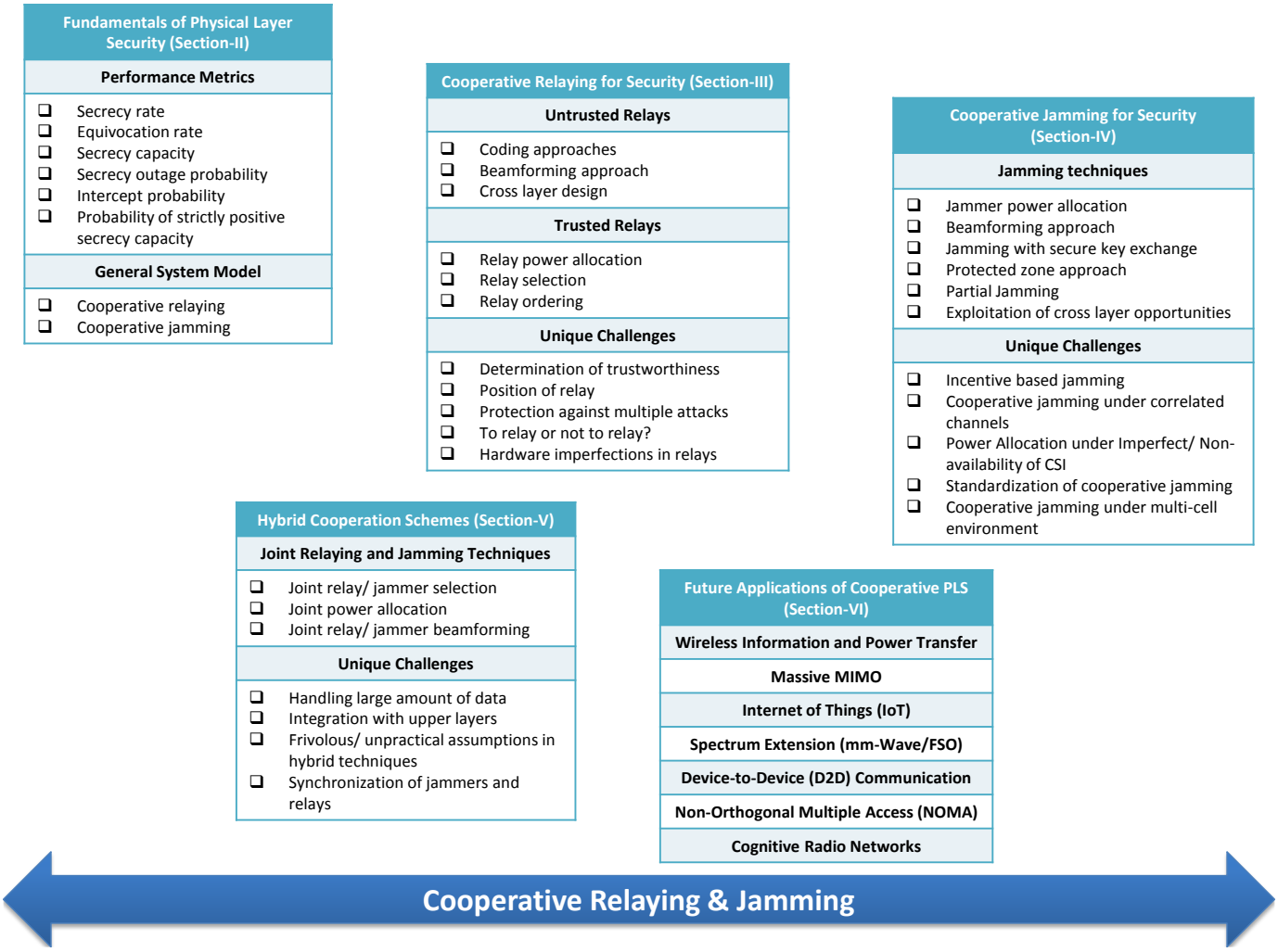


Fig. 2: Taxonomy of cooperative relaying and jamming strategies.

7) Probability of Strictly Positive Secrecy Capacity: Probability of strictly positive secrecy capacity (SPSC) is the probability that the secrecy capacity C_{sec} remains higher than 0 [43], [44], which is given as

$$P_{SPSC} = \Pr(C_{sec} > 0). \tag{12}$$

B. General System Model

Figure 3 presents a generalized cooperative PLS system model. In this model, source S_1 transmits a signal to destination S_2, in the presence of multiple eavesdroppers $\mathbf{E}$ and intermediate helper nodes $\mathbf{H}$, where $\mathbf{E} = \{E_m | m = 1, 2, ...M\}$ and $\mathbf{H} = \{H_k | k = 1, 2, ...K\}$. Note that a helper node can act as a relay, or a jammer, or both[1]. The helper nodes can be adaptively selected to play different roles based on their location. For instance, the nodes closer to the source can relay messages to the destinations. It can otherwise act as jammer. Both cases are now individually discussed.

[1]Since the helper node requires at least two antennas to act as a relay and jammer simultaneously. For the sake of brevity, we only perform derivations for the case where helper node performs either relaying or jamming.

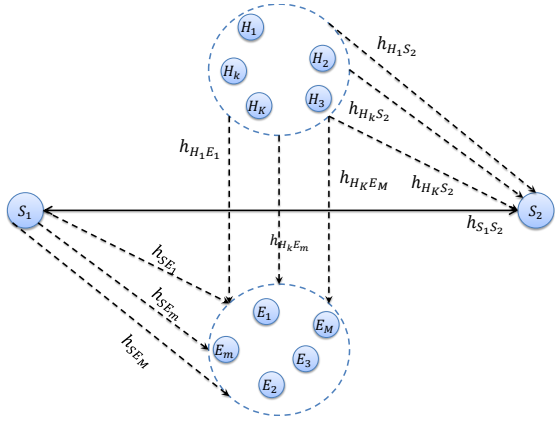


Fig. 3: System model.

1) Cooperative Relaying: There are numerous advantages of introducing relays in the network. Relays can be deployed in areas where the usual backhaul solutions are either unavailable or too expensive. Relaying is also a feasible solution when site acquisition for base station (BS) deployment is a problem. Moreover, relay networks can be deployed and removed easily,

TABLE II: List of acronyms.

Acronym	Full form
AF	Amplify and forward
AF-CS	Amplify and forward compressed sensing
AN	Artificial noise
ANP	Artificial noise aided precoding
AS	Antenna selection
BER	Bit error rate
CB	Cooperative beamforming
CDA	Conventional distributed algorithm
CF	Compress and forward
CI	Channel inversion
CJ	Cooperative jamming
CR	Cognitive radio
CTF	Compute and forward
CUE	Cellular user equipment
D2D	Device-to-device
DAJB	Destination-assisted jamming and beamforming
DBJ	Destination based jamming
DF	Decode and Forward
DTS	Direct transmission scheme
DUM	Deterministic uncertainty model
EB	Eigen-beamforming
EGA	Evolutionary game algorithm
EH	Energy harvesting
FD	Full-duplex
FJaUPS	Friendly jammer-assisted user pair selection
FSO	Free space optical
GSVD	Generalized singular value decomposition
HD	Half duplex
HJ	Harvest and jam
ID	Information decoding
IoT	Internet of things
IPA	Information processing approach
KKT	Karush-Kuhn-Tucker
LoS	Line of sight
LP	Linear programming
M2M	Machine-to-machine
MCSJ	Multichannel single jammer
MF	Modulo-and-forward
MIMO	Multiple-input multiple-output
MISO	Multiple-input single-output
MO-SDP	Monotonic optimization and the semi-definite programming
MPSRM	Minimum peruser secrecy rate maximization
MRC	Maximum ratio combining
MRT	Maximum-ratio transmission
MTC	Machine type communication
NBG	Nash bargaining game
NOMA	Non-orthogonal multiple access
OFDM	Orthogonal frequency division multiplexing
OP-SRM	Outage probability based secrecy rate maximization
PDA	Pragmatic distributed algorithm
PLS	Physical layer security
PS	Power splitting
RCI	Regularize channel inversion
RTS	Relay transmission scheme
SC	Selection combining
SCMJ	Single-channel multijammer
SDP	Semi-definite program
SDR	Semi-definite relaxation
SIC	Successive interference cancellation
SIMO	Single-input multiple-output
SINR	Signal-to-interference-and-noise ratio
SNR	Signal-to-noise ratio
SOP	Secrecy outage probability
SOCP	Second-order convex cone programming
SPCA	Sequential parametric convex approximation
SPSC	Strictly positive secrecy capacity
SRM	Secrecy rate maximization
SSRM	Secrecy sum rate maximization
SUM	Stochastic uncertainty model
SWIPT	Simultaneous wireless information and power transfer
TS	Time switching
TTPM	Total transmit power minimization
UAV	Unmanned aerial vehicles
UE	User equipment
WARP	Wireless open-access research platform
WC-SRM	Worst case secrecy rate maximization
WNCF	Weighted normalized cost function
ZF	Zero forcing

as compared to conventional cellular infrastructure [45]. By deploying relays near the cell edge, the throughput of users can be significantly improved. The deployment of relay networks in areas with low signal levels can result in higher SNRs for the surrounding users, which increases their achievable data rates. In scenarios where several user equipment move in a group (e.g. in a train), a co-located relay can provide improved mobility performance for that group of users.

Typically, relaying involves two phases for transmitting a message from the source to the destination: in the first phase, the message is broadcast from the source to the relay and the destination [46]. During the second phase, the relay node transmits its received message to the destination using a specific protocol, e.g., amplify-and-forward (AF) [47], compress-and-forward (CF) [48], compute-and-forward (CTF) [49], or decode-and-forward (DF) [50]. According to the AF protocol, the relay transmits a scaled version of its received signal. For the CF protocol, the relay compresses the received message before retransmitting it to the destination. In a multiuser scenario, the CTF protocol allows the relay to decode the linear combination of transmitted messages, received from a noisy observation of the channel, which is then passed on to the destination. The destination solves for its desired messages after it has received a sufficient number of linear combinations. In the DF protocol, the relay first decodes the received message and then re-encodes the signal for transmission to the destination [46]. It is pertinent to note that while the AF protocol is simpler to implement, as compared to DF, CTF and CF, its main disadvantage is the amplification of noise in addition to the received signal. The DF protocol provided its best performance when the relay is positioned near the source, or in the case of good channel conditions.

Based on the transmission and reception capability, there are two types of relays: half-duplex (HD) relays [51], [52], [53] and full-duplex (FD) relays [54], [55], [56]. A HD relay needs two orthogonal channel uses to transmit and receive information, whereas a FD relay can simultaneously transmit and receive information, allowing the spectrum to be more efficiently utilized. The FD relaying mode also requires effective mitigation of self-interference at the relay caused by the significant power difference between the received and transmitted signals, assuming identical antenna gains [54]. Despite its lower spectral efficiency, the HD relays are preferred in practical systems, due to their low complexity and ease of implementation [57].

As discussed earlier, the transmission takes place in two phases by dividing a single block of time into two time-slots. However, this can vary for different relaying techniques and protocols. The secrecy capacity under different relaying protocols is listed in Table III.

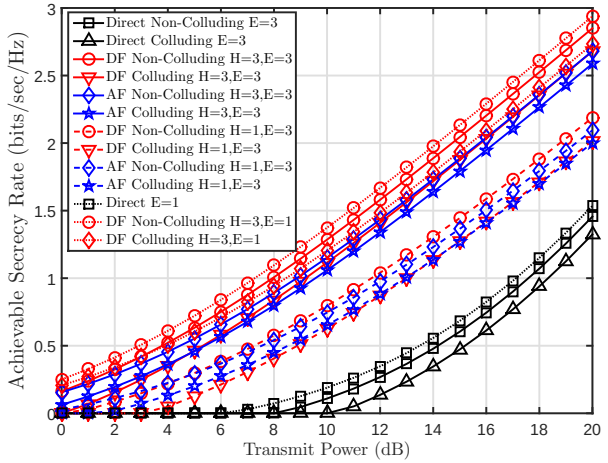


Fig. 4: Achievable secrecy rate for different secure cooperative relaying scenarios.

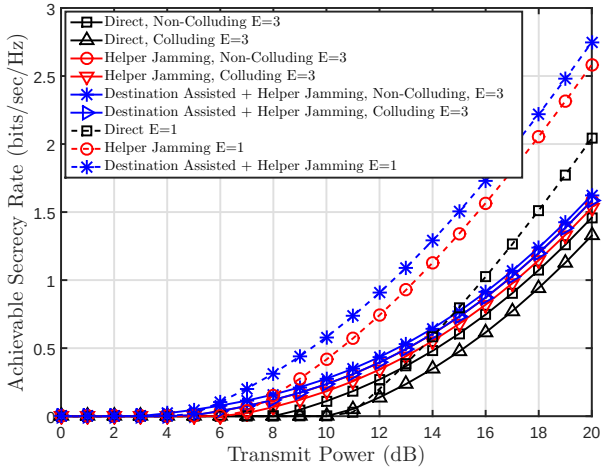


Fig. 5: Achievable secrecy rate for different secure cooperative jamming scenarios.

To provide further insights on the impact of different relaying protocols, Figure 4 plots the achievable secrecy rate for different HD relaying protocols, as a function of the main link's average transmit power. The relaying performance is benchmarked against the direct communication scheme. From Figure 4, it can be observed that the achievable secrecy rate generally increases with an increase in the transmit power. This increase in the secrecy rate is the lowest for direct transmission and is the highest for DF relaying. More specifically, for the direct transmission case, the secrecy rate increases as the number of eavesdroppers decreases from 3 to 1. For the multiple eavesdroppers case, the secrecy rate for non-colluding eavesdroppers is more for the colluding eavesdroppers case. Similar trends can be observed for AF and DF relaying schemes. Among DF and AF protocols, the largest secrecy rate is achieved for DF under non-colluding eavesdropping conditions. When H=3, we consider the optimal relay selection scheme [41] in which a helper node is selected, based on the CSI of both the source-relay and relay-destination links. In general, the figure shows that the secrecy rate is higher when H>E and vice versa, for both AF and DF protocols. However, at lower values of the transmit power, AF outperforms DF in terms of secrecy rate when H<E. Similar trends were also reported in [58].

2) Cooperative Jamming: Although interference is traditionally considered to be undesirable for network operations, it can be leveraged for securing wireless communication links. The most prominent application is cooperative jamming [66], [67], wherein a helper node may sacrifice its entire rate, in order to create interference at the eavesdropper to degrade its performance. Depending on the design considerations, the jamming signals can be of different types. For instance, Gaussian noise, which is similar to additive noise, degrades the signal of both the legitimate and the eavesdropper nodes. In contrast, it is possible to generate a jamming signal to the legitimate node, resulting in only adversely affect the eavesdropper's signal reception [68]. However, this type of jamming requires complex interference cancellation at the legitimate receiver to decode the codeword. Additionally, signals from other legitimate transmitters can also be used to degrade the eavesdropper's signal-to-interference ratio. However, such jamming scenarios are difficult to implement due to time synchronization requirements between the multiple transmitting pairs.

In this case, the helper nodes do not relay information but transmit jamming signals to confuse the eavesdropper. The noise is added by the helper nodes in a controlled manner, causing the noise to be nullified at the destination. This results in increasing the secrecy capacity due to degradation of the received signal at the eavesdroppers. A list of commonly used cooperative jamming techniques along with their secrecy capacity expressions are given in Table IV.

Figure 5 compares the achievable secrecy rate under different jamming conditions for increasing values of the main link's average transmit power. One can observe from the figure that the lowest secrecy rate is achieved for the direct transmission case, which has no jamming by either the helper or the destination node. Moreover, in the direct transmission case, the largest secrecy rate is achieved when there is only a single eavesdropper. We consider that a total of 3 helper nodes exist in the network and the best jammer is selected based on the CSI of the jammer-eavesdropper link. It can be seen that the jamming can help in improving the secrecy performance of the system and proves to be more effective against the non-colluding eavesdroppers. Furthermore, the destination assisted jamming along with the jamming from helper nodes, can also provide significant performance improvements against colluding and non-colluding eavesdroppers. Interestingly, it can be seen from the figure that more performance gains are achieved for destination & helper-assisted jamming when E=1. However, as E increases from 1 to 3, the secrecy rates for helper jamming and destination & helper-assisted jamming are similar to each other, which suggests that the impact of jamming reduces with an increase in the number of eavesdroppers.

TABLE III: Secrecy capacity for various cooperative relaying protocols.

Relay Type	**One/ Two Way**	**Relaying Proto-col**	**Eavesdropper(s)**	**Assumptions**	**Secrecy Capacity**
HD	One Way	AF	Non-Colluding [59]	(1)(2)(4)(6)	$C_{\text{sec}} = \frac{1}{2}\log_2\left[\frac{1+\max_{k\in K}\left\{\frac{P\|h_{S_1}H_k\|^2 P\|h_{H_k}S_2\|^2}{P\|h_{S_1}H_k\|^2+P\|h_{H_k}S_2\|^2+N_0}\right\}}{1+\max_{m\in M}\left\{\frac{P\|h_{S_1}E_m\|^2}{N_0}+\frac{P\|h_{S_1}H_k\|^2 P\|h_{H_k}E_m\|^2}{P\|h_{S_1}H_k\|^2+P\|h_{H_k}E_m\|^2+N_0}\right\}}\right]$
			Colluding [60]	(1)(2)(4)	$C_{\text{sec}} = \frac{1}{2}\log_2\left[\frac{1+\max_{k\in K}\left\{\frac{P\|h_{S_1}H_k\|^2 P\|h_{H_k}S_2\|^2}{P\|h_{S_1}H_k\|^2+P\|h_{H_k}S_2\|^2+N_0}\right\}}{1+\sum_{m=1}^{M}\left\{\frac{P\|h_{S_1}E_m\|^2}{N_0}+\frac{P\|h_{S_1}H_k\|^2 P\|h_{H_k}E_m\|^2}{P\|h_{S_1}H_k\|^2+P\|h_{H_k}E_m\|^2+N_0}\right\}}\right]$
		DF	Non-Colluding [61]	(1)(2)(4)	$C_{\text{sec}} = \frac{1}{2}\log_2\left[\frac{1+\max_{k\in K}\left\{\min\left\{\frac{P\|h_{S_1}H_k\|^2}{N_0},\frac{P\|h_{H_k}S_2\|^2}{N_0}\right\}\right\}}{1+\max_{m\in M}\left\{\frac{P\|h_{S_1}E_m\|^2}{N_0}+\frac{P\|h_{H_k}E_m\|^2}{N_0}\right\}}\right]$
			Colluding [61]	(1)(2)(4)	$C_{\text{sec}} = \frac{1}{2}\log_2\left[\frac{1+\max_{k\in K}\left\{\min\left\{\frac{P\|h_{S_1}H_k\|^2}{N_0},\frac{P\|h_{H_k}S_2\|^2}{N_0}\right\}\right\}}{1+\sum_{m=1}^{M}\left\{\frac{P\|h_{S_1}E_m\|^2}{N_0}+\frac{P\|h_{H_k}E_m\|^2}{N_0}\right\}}\right]$
	Two Way	AF	Non-Colluding [62]	(1)(2)(3)(5)(6)	$C_{\text{sec}} = \log_2\left[\min\left\{\frac{1+\max_{k\in K}\left\{\frac{P\|h_{S_1}H_k\|^2 P\|h_{H_k}S_2\|^2}{P\|h_{S_1}H_k\|^2+P\|h_{H_k}S_2\|^2+N_0}\right\}}{1+\max_{m\in M}\left\{\frac{P\|h_{S_1}E_m\|^2}{N_0}+\frac{P\|h_{S_1}H_k\|^2 P\|h_{H_k}E_m\|^2}{P\|h_{S_1}H_k\|^2+P\|h_{H_k}E_m\|^2+N_0}\right\}}, \frac{1+\max_{k\in K}\left\{\frac{P\|h_{S_2}H_k\|^2 P\|h_{H_k}S_1\|^2}{P\|h_{S_2}H_k\|^2+P\|h_{H_k}S_1\|^2+N_0}\right\}}{1+\max_{m\in M}\left\{\frac{P\|h_{S_2}E_m\|^2}{N_0}+\frac{P\|h_{S_2}H_k\|^2 P\|h_{H_k}E_m\|^2}{P\|h_{S_2}H_k\|^2+P\|h_{H_k}E_m\|^2+N_0}\right\}}\right\}\right]$
			Colluding	(1)(2)(3)(5)	$C_{\text{sec}} = \log_2\left[\min\left\{\frac{1+\max_{k\in K}\left\{\frac{P\|h_{S_1}H_k\|^2 P\|h_{H_k}S_2\|^2}{P\|h_{S_1}H_k\|^2+P\|h_{H_k}S_2\|^2+N_0}\right\}}{1+\sum_{m=1}^{M}\left\{\frac{P\|h_{S_1}E_m\|^2}{N_0}+\frac{P\|h_{S_1}H_k\|^2 P\|h_{H_k}E_m\|^2}{P\|h_{S_1}H_k\|^2+P\|h_{H_k}E_m\|^2+N_0}\right\}}, \frac{1+\max_{k\in K}\left\{\frac{P\|h_{S_2}H_k\|^2 P\|h_{H_k}S_1\|^2}{P\|h_{S_2}H_k\|^2+P\|h_{H_k}S_1\|^2+N_0}\right\}}{1+\sum_{m=1}^{M}\left\{\frac{P\|h_{S_2}E_m\|^2}{N_0}+\frac{P\|h_{S_2}H_k\|^2 P\|h_{H_k}E_m\|^2}{P\|h_{S_2}H_k\|^2+P\|h_{H_k}E_m\|^2+N_0}\right\}}\right\}\right]$
		DF	Non-Colluding [63]	(1)(2)(3)(5)	$C_{\text{sec}} = \log_2\left[\min\left\{\frac{1+\max_{k\in K}\left\{\min\left\{\frac{P\|h_{S_1}H_k\|^2}{N_0},\frac{P\|h_{H_k}S_2\|^2}{N_0}\right\}\right\}}{1+\max_{m\in M}\left\{\frac{P\|h_{S_1}E_m\|^2}{N_0}+\frac{P\|h_{H_k}E_m\|^2}{N_0}\right\}}, \frac{1+\max_{k\in K}\left\{\min\left\{\frac{P\|h_{S_2}H_k\|^2}{N_0},\frac{P\|h_{H_k}S_1\|^2}{N_0}\right\}\right\}}{1+\max_{m\in M}\left\{\frac{P\|h_{S_2}E_m\|^2}{N_0}+\frac{P\|h_{H_k}E_m\|^2}{N_0}\right\}}\right\}\right]$
			Colluding	(1)(2)(3)(5)	$C_{\text{sec}} = \log_2\left[\min\left\{\frac{1+\max_{k\in K}\left\{\min\left\{\frac{P\|h_{S_1}H_k\|^2}{N_0},\frac{P\|h_{H_k}S_2\|^2}{N_0}\right\}\right\}}{1+\sum_{m=1}^{M}\left\{\frac{P\|h_{S_1}E_m\|^2}{N_0}+\frac{P\|h_{H_k}E_m\|^2}{N_0}\right\}}, \frac{1+\max_{k\in K}\left\{\min\left\{\frac{P\|h_{S_2}H_k\|^2}{N_0},\frac{P\|h_{H_k}S_1\|^2}{N_0}\right\}\right\}}{1+\sum_{m=1}^{M}\left\{\frac{P\|h_{S_2}E_m\|^2}{N_0}+\frac{P\|h_{H_k}E_m\|^2}{N_0}\right\}}\right\}\right]$
FD	One Way	AF	Non-Colluding [64]	(1)(2)(4)(6)	$C_{\text{sec}} = \frac{1}{2}\log_2\left[\frac{1+\max_{k\in K}\left\{\frac{\frac{P\|h_{S_1}H_k\|^2}{P\|h_{H_k}\bar{H}_k\|^2+1}P\|h_{H_k}S_2\|^2}{\frac{P\|h_{S_1}H_k\|^2}{P\|h_{H_k}\bar{H}_k\|^2+1}+P\|h_{H_k}S_2\|^2+N_0}\right\}}{1+\max_{m\in M}\left\{\frac{P\|h_{S_1}E_m\|^2}{N_0}+\frac{P\|h_{H_k}E_m\|^2}{N_0}\right\}}\right]$
			Colluding	(1)(2)(4)	$C_{\text{sec}} = \frac{1}{2}\log_2\left[\frac{1+\max_{k\in K}\left\{\frac{\frac{P\|h_{S_1}H_k\|^2}{P\|h_{H_k}\bar{H}_k\|^2+1}P\|h_{H_k}S_2\|^2}{\frac{P\|h_{S_1}H_k\|^2}{P\|h_{H_k}\bar{H}_k\|^2+1}+P\|h_{H_k}S_2\|^2+N_0}\right\}}{1+\sum_{m=1}^{M}\left\{\frac{P\|h_{S_1}E_m\|^2}{N_0}+\frac{P\|h_{H_k}E_m\|^2}{N_0}\right\}}\right]$

		DF	Non-Colluding [65]	(1)(2)(4)	$C_{\text{sec}} = \frac{1}{2}\log_2 \left[\frac{1+\max_{k\in K}\left\{\min\left\{\frac{P\|h_{S_1}H_k\|^2}{P\|h_{H_k}\bar{H}_k\|^2+N_0}, \frac{P\|h_{H_k}S_2\|^2}{N_0}\right\}\right\}}{1+\max_{m\in M}\left\{\frac{P\|h_{S_1}E_m\|^2}{N_0}+\frac{P\|h_{H_k}E_m\|^2}{N_0}\right\}} \right]$
			Colluding	(1)(2)(4)	$C_{\text{sec}} = \frac{1}{2}\log_2 \left[\frac{1+\max_{k\in K}\left\{\min\left\{\frac{P\|h_{S_1}H_k\|^2}{P\|h_{H_k}\bar{H}_k\|^2+N_0}, \frac{P\|h_{H_k}S_2\|^2}{N_0}\right\}\right\}}{1+\sum_{m=1}^{M}\left\{\frac{P\|h_{S_1}E_m\|^2}{N_0}+\frac{P\|h_{H_k}E_m\|^2}{N_0}\right\}} \right]$
	Two Way	AF	Non-Colluding	(1)(2)(3)(5)(6)	$C_{\text{sec}} = \log_2\Bigg[\min\Bigg\{ \frac{1+\max_{k\in K}\left\{ \frac{\frac{P\|h_{S_1}H_k\|^2}{P\|h_{H_k}\bar{H}_k\|^2+1}P\|h_{H_k}S_2\|^2}{\frac{P\|h_{S_1}H_k\|^2}{P\|h_{H_k}\bar{H}_k\|^2+1}+P\|h_{H_k}S_2\|^2+N_0}\right\}}{1+\max_{m\in M}\left\{\frac{P\|h_{S_1}E_m\|^2}{N_0}+\frac{P\|h_{H_k}E_m\|^2}{N_0}\right\}}, \frac{1+\max_{k\in K}\left\{ \frac{\frac{P\|h_{S_2}H_k\|^2}{P\|h_{H_k}\bar{H}_k\|^2+1}P\|h_{H_k}S_1\|^2}{\frac{P\|h_{S_2}H_k\|^2}{P\|h_{H_k}\bar{H}_k\|^2+1}+P\|h_{H_k}S_1\|^2+N_0}\right\}}{1+\max_{m\in M}\left\{\frac{P\|h_{S_2}E_m\|^2}{N_0}+\frac{P\|h_{H_k}E_m\|^2}{N_0}\right\}} \Bigg\}\Bigg]$
			Colluding	(1)(2)(3)(5)	$C_{\text{sec}} = \log_2\Bigg[\min\Bigg\{ \frac{1+\max_{k\in K}\left\{ \frac{\frac{P\|h_{S_1}H_k\|^2}{P\|h_{H_k}\bar{H}_k\|^2+1}P\|h_{H_k}S_2\|^2}{\frac{P\|h_{S_1}H_k\|^2}{P\|h_{H_k}\bar{H}_k\|^2+1}+P\|h_{H_k}S_2\|^2+N_0}\right\}}{1+\sum_{m=1}^{M}\left\{\frac{P\|h_{S_1}E_m\|^2}{N_0}+\frac{P\|h_{H_k}E_m\|^2}{N_0}\right\}}, \frac{1+\max_{k\in K}\left\{ \frac{\frac{P\|h_{S_2}H_k\|^2}{P\|h_{H_k}\bar{H}_k\|^2+1}P\|h_{H_k}S_1\|^2}{\frac{P\|h_{S_2}H_k\|^2}{P\|h_{H_k}\bar{H}_k\|^2+1}+P\|h_{H_k}S_1\|^2+N_0}\right\}}{1+\sum_{m=1}^{M}\left\{\frac{P\|h_{S_2}E_m\|^2}{N_0}+\frac{P\|h_{H_k}E_m\|^2}{N_0}\right\}} \Bigg\}\Bigg]$
		DF	Non-Colluding	(1)(2)(3)(5)	$C_{\text{sec}} = \log_2\Bigg[\min\Bigg\{ \frac{1+\max_{k\in K}\left\{\min\left\{\frac{P\|h_{S_1}H_k\|^2}{P\|h_{H_k}\bar{H}_k\|^2+N_0}, \frac{P\|h_{H_k}S_2\|^2}{N_0}\right\}\right\}}{1+\max_{m\in M}\left\{\frac{P\|h_{S_1}E_m\|^2}{N_0}+\frac{P\|h_{H_k}E_m\|^2}{N_0}\right\}}, \frac{1+\max_{k\in K}\left\{\min\left\{\frac{P\|h_{S_2}H_k\|^2}{P\|h_{H_k}\bar{H}_k\|^2+N_0}, \frac{P\|h_{H_k}S_1\|^2}{N_0}\right\}\right\}}{1+\max_{m\in M}\left\{\frac{P\|h_{S_2}E_m\|^2}{N_0}+\frac{P\|h_{H_k}E_m\|^2}{N_0}\right\}} \Bigg\}\Bigg]$
			Colluding	(1)(2)(3)(5)	$C_{\text{sec}} = \log_2\Bigg[\min\Bigg\{ \frac{1+\max_{k\in K}\left\{\min\left\{\frac{P\|h_{S_1}H_k\|^2}{P\|h_{H_k}\bar{H}_k\|^2+N_0}, \frac{P\|h_{H_k}S_2\|^2}{N_0}\right\}\right\}}{1+\sum_{m=1}^{M}\left\{\frac{P\|h_{S_1}E_m\|^2}{N_0}+\frac{P\|h_{H_k}E_m\|^2}{N_0}\right\}}, \frac{1+\max_{k\in K}\left\{\min\left\{\frac{P\|h_{S_2}H_k\|^2}{P\|h_{H_k}\bar{H}_k\|^2+N_0}, \frac{P\|h_{H_k}S_1\|^2}{N_0}\right\}\right\}}{1+\sum_{m=1}^{M}\left\{\frac{P\|h_{S_2}E_m\|^2}{N_0}+\frac{P\|h_{H_k}E_m\|^2}{N_0}\right\}} \Bigg\}\Bigg]$

Assumptions: (1) Block fading model (2) Availability of global CSI at nodes (3) Worst case eavesdropping - such that eavesdropper has already decoded message of one of the nodes (4) Single block of time divided in two time slots (5) Single block of time divided into three time slots (6) Variable gain AF

III. Cooperative Relaying for Security

Lately, secure communication via relays has drawn much attention. Since these relays are distributed, the geographical distance of communication between the source and destination can still be decreased which results in the secrecy performance being improved. The achievable secrecy rate and secrecy capacity have been evaluated under different source-relay-eavesdropper scenarios. In fact, based on their role in the network, these relays can be a trusted entity or completely stranger (untrusted) to the communicating parties. Therefore, various modalities have been proposed to provide security using cooperative strategies for single and multiple-antenna devices as shown in Table V.

A. Untrusted Relays

In many practical cases, even when the external eavesdropper is not present in the network, secure communication between two nodes, using an intermediate relay, can be a concern. The source and the destination may want to keep their communication secret from the relay despite its willingness to cooperate [69]. This model has critical importance in government and defense intelligence networks where all users do not have the same access rights [70]. Also, if the relay belongs to a different network, its access to the information of the nodes for the other network will not be granted. Several studies indicate that it is possible to securely transfer messages from the a source to a destination using intermediate *untrusted relays* [71], [72], [73], [74], [75], [76]. In [77], the diversity

TABLE IV: Secrecy capacity for different cooperative jamming schemes.

Jamming Technique	**No. of Jammers**	**Eavesdropper(s)**	**Assumptions**	**Secrecy Capacity**
Jammer Selection	Multiple	Non-Colluding	(1)(2)(3)(5)	$C_{\text{sec}} = \log_2 \left[\frac{1+\frac{P\lvert h_{S_1S_2}\rvert^2}{N_0}}{1+\max_{m\in M}\left\{ \frac{P\lvert h_{S_1E_m}\rvert^2}{\max_{k\in K}\left\{P\lvert h_{H_kE_m}\rvert^2\right\}+N_0}\right\}} \right]$
		Colluding	(1)(2)(3)(5)	$C_{\text{sec}} = \log_2 \left[\frac{1+\frac{P\lvert h_{S_1S_2}\rvert^2}{N_0}}{1+\sum_{m=1}^{M}\left\{ \frac{P\lvert h_{S_1E_m}\rvert^2}{\max_{k\in K}\left\{P\lvert h_{H_kE_m}\rvert^2\right\}+N_0}\right\}} \right]$
Multiple Antenna	Single	Non-Colluding	(1)(2)(4)	$C_{\text{sec}} = \log_2 \left[\frac{1+\frac{P\lvert h_{S_1S_2}\rvert^2}{\lvert w^{\perp}h_{H_kS_2}\rvert^2+N_0}}{1+\max_{m\in M}\left\{ \frac{P\lvert h_{S_1E_m}\rvert^2}{\lvert w^{\perp}h_{H_kE_m}\rvert^2+N_0}\right\}} \right]$
		Colluding	(1)(2)(4)	$C_{\text{sec}} = \log_2 \left[\frac{1+\frac{P\lvert h_{S_1S_2}\rvert^2}{\lvert w^{\perp}h_{H_kS_2}\rvert^2+N_0}}{1+\sum_{m=1}^{M}\left\{ \frac{P\lvert h_{S_1E_m}\rvert^2}{\lvert w^{\perp}h_{H_kE_m}\rvert^2+N_0}\right\}} \right]$
Destination Assisted	Single	Non-Colluding	(1)(2)(4)(5)	$C_{\text{sec}} = \log_2 \left[\frac{1+\frac{P\lvert h_{S_1S_2}\rvert^2}{P\lvert h_{S_2S_2}\rvert^2+N_0}}{1+\max_{m\in M}\left\{ \frac{P\lvert h_{S_1E_m}\rvert^2}{P\lvert h_{S_2E_m}\rvert^2+\max_{k\in K}\left\{P\lvert h_{H_kE_m}\rvert^2\right\}+N_0}\right\}} \right]$
		Colluding	(1)(2)(4)(5)	$C_{\text{sec}} = \log_2 \left[\frac{1+\frac{P\lvert h_{S_1S_2}\rvert^2}{P\lvert h_{S_2S_2}\rvert^2+N_0}}{1+\sum_{m=1}^{M}\left\{ \frac{P\lvert h_{S_1E_m}\rvert^2}{P\lvert h_{S_2E_m}\rvert^2+\max_{k\in K}\left\{P\lvert h_{H_kE_m}\rvert^2\right\}+N_0}\right\}} \right]$

Assumptions: (1) Block fading model (2) Availability of global CSI at nodes (3) Jamming signal canceled at destination (4) Jamming signal acting as interference at the destination (5) Best jamming node selection

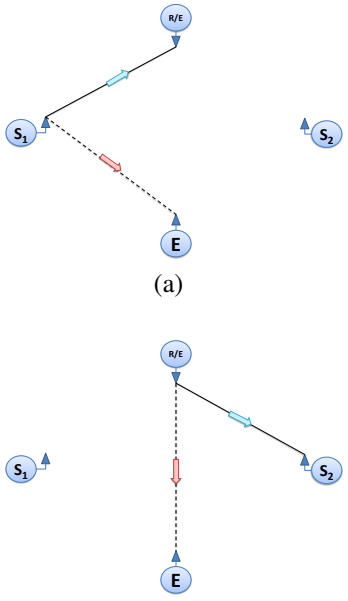


Fig. 6: Secure communication with untrusted relaying (a) relay reception (b) relay transmission.

order and capacity scaling to securely forward the information in untrusted relaying environment is investigated. A more realistic scenario was considered in [78] by introducing trust degree-based cooperation. A typical scenario, where a node can act as a relay and an eavesdropper is given in Figure 6. Here, the communication takes place in two time slots. During the first time slot, S_1 broadcasts its message to the untrusted relay R/E and eavesdropper E while S_2 may not receive the broadcast signal, due to deep fading. Generally, the untrusted relay can use either the DF or the AF protocol to forward its message to S_2 in the second time slot. However, the AF protocol is generally preferred in this case as S_1 may not want an untrusted relay to decode the message meant for S_2. The same signal is also overheard by E in the second time slot, and E may decide to combine or to use any one of the signals to decode the message of S_1. In order to prevent E and R/E from decoding the secret message, several PLS approaches have been provided in the literature. Let us now briefly discuss some of these strategies for providing link security in untrusted relaying scenarios.

1) Coding Approaches: In the paradigm of untrusted relaying, secure transmission was studied in a multi-hop scenario in [79]. In this context, it was assumed that the direct link between the source and the destination does not exist and the communication between them is only possible through an

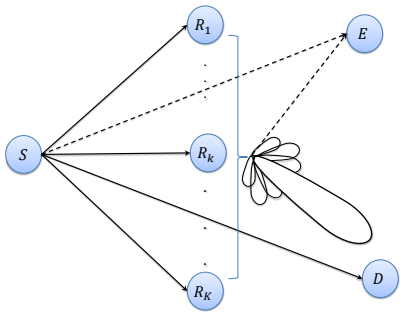


Fig. 7: Illustration of K relaying nodes performing cooperative beamforming.

intermediate untrusted relay. It was also assumed that each node could only communicate with its immediate neighbor to relay the information to the destination. This study focuses on nested lattice codes and used CTF protocol to relay information.

2) Beamforming Approach: Secure beamforming techniques can be used for providing link security as shown in Figure 7. Particularly, beamforming is used to transmit signals to a specific user, resulting in degradation of SNR of the same signal at any other user. A MIMO relaying system was considered in [80] for transmission using AF protocol. A two-hop scenario was considered where the intermediate relay was not trusted. Specifically, the following two conditions were considered.

- Non-collaborative scheme: The intermediate node is assumed to be an external node.
- Collaborative scheme: The relay re-transmits using beamforming at relay.

The results presented by the authors show that collaborative scheme outperforms the non-collaborative scheme in terms of achievable secrecy when the SNR of the source-relay and relay-destination links were low. In addition, the proposed schemes ensure higher secrecy, as compared to conventional beamforming.

3) Cross Layer Design: When the communication is not possible between the source and destination without the intermediate untrusted relays, then an appropriate solution is distribution of untrusted relays into collaborative and non-collaborative relays [81]. In particular, if the source has to transfer information, the access of intermediate nodes to the information must be minimized. When any untrusted relay receives the information, all other relays are assumed to overhear that information. The entire information is divided into m data streams and then the associated data rates, for each stream, can be given as $R_1, R_2, R_3, ..., R_m$. The desired transmission rate from a source to a destination is given as

$$R_t = \sum_{i=1}^{m} R_i \tag{13}$$

In another study [82], the authors proposed to use upper layer security, along with PLS, to improve the secrecy of the data being transferred through untrusted relays. The study showed that for AF relays, perfect secrecy of information was attainable, whereas for DF protocol, significant amount of information leakage occur.

B. Trusted Relays

In the case of trusted relays, the eavesdroppers and relays are considered to be separate network entities. Some of the common relay-eavesdropper scenarios for HD, FD and successive relaying are provided in Figure 8. It can be seen from the figure that for HD-relaying techniques, the information transmission takes place in two time slots. The direction of communication can be either one-way (i.e., $S_1 \rightarrow R \rightarrow S_2$) or two-way, i.e., $S_1 \longleftrightarrow R \longleftrightarrow S_2$. For both the one-way and two-way cooperative relaying, there are two transmission modes namely the *relay reception mode* for the first time slot and the *relay transmission mode* for the second time slot. Intuitively, for one-way relaying the eavesdropper can receive the same signal during the first and second time slots, which can be exploited to decode the secret message. In case of two-way relaying, the eavesdropper receives the message of S_1 and S_2 in the first time slot and it receives the superimposed signals of S_1 and S_2 from R during the second time slot. For successive relaying, two relays are used to improve the throughput of the system. During the first time slot, S_1 transmits its message to R_1 while R_2 transmits its message to S_2, assuming that R_2 received a message in the previous transmission. During the second time slot, S_1 again broadcasts its message, which is received by R_2 to forward to S_2 in subsequent time slots. If an eavesdropper lies in the communication range of S_1, R_1, and R_2 then successive relaying may prove to be more susceptible to information leakage since the eavesdropper has a better chance of decoding the messages received during two time slots. Despite the hardware complexity of FD communications, it has several advantages over HD communications such as an increased ergodic capacity [118], [119], reduced end-to-end delays [120], reduced feedback delays [121], and improved network secrecy [122], [123]. Based on the usage of frequency band, FD relaying can be divided into two types, i.e., FD-outband relaying and FD-inband relaying, as illustrated in Figure 8 (g) & (h), respectively. The self-interference cancellation techniques play a more vital role in FD-inband relaying, especially in the presence of eavesdroppers. However, the generated interference can act as artificial interference to minimize the leakage of information to the eavesdropper, while simultaneously improving the power efficiency of the system [123], [124]. Some other cooperative relaying strategies are reviewed in the following sub-sections.

1) Relay Power Allocation: The required transmit power is one of the major concerns when a signal is transmitted across the network. A low power signal can increase decoding errors at the destination, due to the signal attenuation from the path loss and fading. In contrast, a signal with high power improves the received signal strength at the intended receiver, at the cost of introducing significant interferences for other receiving nodes. Therefore, optimum allocation of power is important from not only a communication point of view, but also from the secrecy perspective. The problem of optimum power allocation is analyzed in [125] and the authors proposed

TABLE V: Comparative summary of different cooperative relaying protocols.

Relaying Category	Reference	Relaying Scheme	Single / Multiple Antenna	One/ Two-Way Relaying	Solution
Untrusted	[83], [70]	AF & CF	Single Antenna	One-way	Proved that for larger channel gain of the main link, the source does not need to transfer message at higher power as it will improve relay's ability to decode.
	[84]	CTF	Single Antenna	One-way	Decode by linear combination of incoming signals instead of decoding individually
	[85]	CTF	Single Antenna	One-way	Showed that CTF works best with lattice codes to improve secrecy capacity
	[86]	CTF	Multiple Antenna	Two-way	Showed that introduction of multiple antennas at the source nodes and the optimization of the transmit power improves the information security
	[79]	CTF	Single Antenna	One-way	End-to-end secure communication via joint use of wiretap codes, lattice codes, and a network coding scheme
	[73]	AF	Single Antenna	One-way	Proposed a modulo-and-forward (MF) operation at the relay with nested lattice encoding at the source
	[87]	AF	Single Antenna	One-way	Proved that a relay, no matter whether it is chosen as a helper or not, acts as an eavesdropper and the performance of secure communication systems is worse off when the number of relays increases
	[88]	AF	Single Antenna	Two-way	Found that if one node's transmit power is much lower than the other then two-way relaying with AF strategies is the best choice
	[89]	AF	Single Antenna	One-way	Derivation of close-form ergodic secrecy rate as well as the asymptotic expressions
	[80]	AF	Multiple Antenna	One-way	Optimization of transmit covariance matrices for secrecy enhancement
	[90]	AF	Multiple Antenna	Two-way	Optimization of covariance matrices for both relay-aided and direct communications
	[91]	AF	Single Antenna	One-way	Derivation of unified tight approximation and asymptotic expressions for the system secrecy outage probability with outdated CSI
	[87]	AF	Single Antenna	One-way	Derivation of lower bound of the ergodic secrecy capacity
	[83]	AF	Single Antenna	One-way	Derivation of Upper bound of the ergodic secrecy capacity in the presence of a jamming node
	[92]	CTF	Single Antenna	One-way	Derivation of genie-aided outer bounds on the secrecy rate regions
Trusted	[93]	NF, AF, DF	Single Antenna	One-way	Investigation of optimal relay location between the source and destination in a relaying network
	[58]	CF, AF, DF	Single Antenna	One-way	Derivation of optimal power allocation in closed-form
	[94]	DF	Single Antenna	One-way	Proposed achieved secrecy regions using a Cover and El Gamal's CF scheme
	[95]	AF	Multiple Antenna	One-way	Compared the benchmark nulling solution with local nulling
	[96]	DF, AF	Multiple Antenna	One-way	Compare secrecy outage capacity of AF and DF protocols
	[97]	DF	Multiple Antenna	One-way	Design an optimal relay beamformer to maximize secrecy rate and minimize transmit power, respectively
	[98]	DF	Multiple Antenna	One-way	Propose a joint generalized singular value decomposition (GSVD) precoding at the source and ZF-SVD precoding at relay and power allocation scheme
	[61]	DF	Single Antenna	One-way	Revised Bellman Ford algorithm for providing a secure route in multihop scenario
	[99]	DF	Single Antenna	One way	Maximization of secrecy rate under strict delay constraint
	[100]	DF	Multiple Antenna	One-way	Analyzing impact of jamming on bit error rate (BER) and throughput under imperfect CSI
	[101]	AF	Multiple Antenna	One-way	Present secrecy rate maximization beamforming and null space beamforming for cooperative relays
	[102]	AF	Multiple Antenna	One-way	Design a robust relay beamformer, including optimal rank-one, MF, and ZF beamformer
	[103]	AF	Multiple Antenna	One-way	Joint transmit/receive beamforming at relay
	[104]	AF	Multiple Antenna	One-way	Propose a joint GSVD precoding at the source and ZF-SVD precoding at relay and a power allocation scheme
	[74]	AF	Multiple Antenna	One-way	Designed destination aided precoding and optimized the performance using iterative algorithm
	[105]	AF	Multiple Antenna	One-way	Optimal power allocation to maximize the secrecy rate in FD relays
	[106]	DF	Single Antenna	Two-way	Derivation of lower and upper bounds on the perfect secrecy rate
	[107], [108]	DF	Single Antenna	One-way	Analysis of reliability and security tradeoff
	[109]	DF	Multiple Antenna	One-way	Secrecy analysis for multi-antenna and multiple relays
	[110]	DF	Single Antenna	Two-way	Provided closed-form SOP expression under κ-μ shadow fading.
	[111]	DF	Single Antenna	One-way	Analysis of reliability and security tradeoff
	[112]	DF	Multiple Antenna	Two-way	Establishment of secrecy capacity regions for discrete memoryless and MIMO Gaussian channels

	[113]	DF	Multiple Antenna	One-way	Proposed SDP relaxation method and a suboptimal criteria of the precoding scheme
	[114]	DF	Multiple Antenna	One-way	Proposed space division multiplexing for allocation of the maximal allowable power
	[115]	DF	Multiple Antenna	One-way	Proposed artificial noise (AN) precoding to minimize the power allocated to information transmissions
	[116]	DF	Multiple Antenna	One-way	Provided three approaches 1) secrecy sum rate maximization (SSRM), 2) total transmit power minimization (TTPM), 3) minimum peruser secrecy rate maximization (MPSRM)
	[113]	DF	Multiple Antenna	One-way	Proposed SDP relaxation method and a suboptimal criteria of the precoding scheme
	[117]	DF	Multiple Antenna	One-way	Proposed smart jamming algorithm for the relay that is not assigned to any pairs to act as a friendly cooperative jammer
	[41]	DF	Multiple Antenna	One-way	Proposed a joint relay and jammer selection scheme to select two or three intermediate nodes to enhance security against Eve

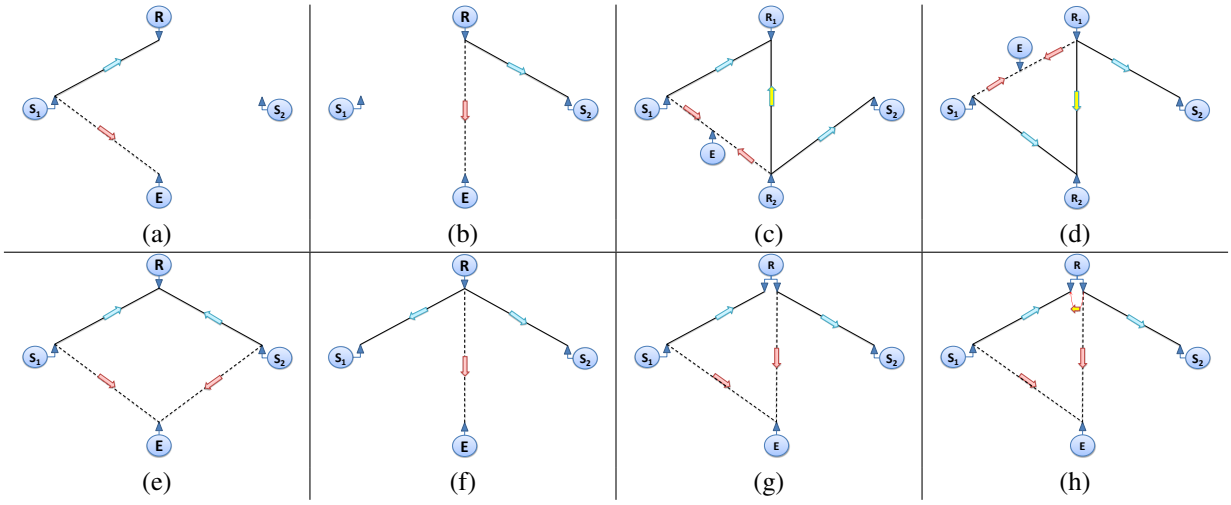


Fig. 8: Different eavesdropping conditions in (a) One-way HD - Relay Reception Mode, (b) One-way HD - Relay Transmission Mode, (c) Successive Relaying - R2 Transmission, (d) Successive Relaying - R1 Transmission, (e) Two-Way HD - Relay Reception Mode, (f) Two-Way HD - Relay Transmission Mode, (g) FD - Outband, (h) FD - Inband.

a convex optimization and one dimensional search method. Generally, the literature concerning power allocation considers total power as a constraint on objective function. A rather better approach is to focus on the power constraint of an individual relay. Thus, the authors in [125] maximize secrecy rate and reduce individual power consumption on the relay. A beamforming vector is formed, which increases secrecy rate subject to individual power constraints.

In [126], the authors emphasized on a technique of orthogonal frequency division multiplexing (OFDM) coordination strategy, based on Nash bargaining game (NBG). The problem of sub-carrier allotment on individual devices is devised on the basis of a bargaining, game between two people to set up fairness in the process. The system model in [126] consists of an OFDM transmission system with two sources, destinations and an adversary. Every node acts as a source as well as a forwarding relay. Then, the allotment of sub-carrier between the coordinating end-systems is obtained through NBG along segment/ frame of evolutionary game algorithm (EGA). Ultimately, the results are corroborated through simulations that show an effective evaluation and gaining improved secrecy rate as compared to direct transmission strategy.

In [127], the authors highlighted that link security methods were aimed to secure the signal, as opposed to securing the data. Since the channel has random nature and cannot be controlled by the users, a design in which channel state is considered essential for the intended channel may not be suitable for many practical scenarios. Their system model was based on AF relaying, where the transmitter used single antennas while the receiver contains multiple antennas. The receiver can perform FD process thus it can send and pick signals simultaneously. The authors then discussed the importance of the CSI for PLS procedures, with current challenges faced by security mechanisms based on CSI. For this purpose, they mentioned three important concepts: spatial domain utilization, transmission of intentional interference and cyclic feature suppression.

Resource allocation under certain constraints can improve the secrecy performance under AF relaying [128]. The authors analyzed PLS issue in OFDMA enabled two-hop model, based on multiple intermediate relays and a passive eavesdropper. The proposed system model in [128] considered dual-hop transmission mode where links from BS to the users and from the BS to an adversary were unknown due to large distance. Thus, all the secret users and the malicious node get information messages merely through relay nodes. Essentially, the sub-carrier allotment to users individually and the power thresholds over different sub-carriers at transmitting nodes

were optimized. Subsequently, a suboptimal solution was derived, supplying significant gain upon the conventional solution. The results of the simulation verified that the proposed scheme supersedes the conventional approach and remarkable improvements were shown against different values of the network parameters.

2) Relay Selection: Another secrecy enhancement criterion is the relay selection in the network. The optimal relay selection policy was adopted for DF protocol in [129] and it was shown to be far better than traditional max-min relay selection. In [108], an opportunistic relay selection policy was used. It has been proven that secrecy outage probability significantly reduces when the number of DF relays increases in the network. Single and multiple relay selection schemes were considered for AF and DF protocols in [41]. In addition to this, diversity order for each scheme was presented in the paper. Buffer-aided relays, for enhancement of PLS and transmission efficiency was considered in [130] for two-hop relay networks.

A combined AF and CF scheme can be used for providing link security using cooperative relaying [131]. Here, the concept of broadcast is considered in a way so, instead of one transmitter and one legitimate receiver, many receivers are present in the network. The DF protocol can only be used if the relay nodes have good channel conditions. A node that serves as a relay may need lower security clearance than the destination. The average probability of error is defined in a sense where the message is decoded in error. At receiver side, the sliding window decoding algorithm is used. A DF relay selection methodology where the main and wiretap links experience correlated fading, was proposed by the authors in [132]. In contrast, the same author proposed a relay selection scheme for correlated AF relaying. Although few other works including [133], [134] have considered secrecy under correlated fading, correlated fading scenarios in Figure 9 can also be explored to provide further insights. Particularly, in Figure 9 (a), the direct link between the source S and D is assumed to be unavailable. The message is transferred with the support of the K intermediate relays and the correlation exists between actual and estimated links. In Figure 9 (b), the source-relay and relay-destination links of the same relay are assumed to be correlated. Moreover, each relay is assumed to experience independent fading. Finally, in Figure 9 (c), correlation exists among source-relay links and among relay-destination links. Also, the links between source-relay and relay-destination are assumed to be independently fading.

By considering high SNR, the authors in [135], [41] analyzed secure communication for perfect decoding at the source relay link. However, this assumption completely ignores the reduction in data rates, due to fading between source relay links. In contrast, the authors in [136], [137], [138] deviate from this assumption by considering imperfect decoding, due to fading between source relay links. All of these papers derive secrecy outage probability expression for DF relaying, whereas, only [136] and [137] consider no direct link and [138] considers direct link between the source and destination as well as focuses on relay selection schemes. Secrecy performance analysis of dual-hop threshold relaying was evaluated in [139] for a single source, single destination, single relay and single eavesdropper scenario. Additionally, closed-form expressions of secrecy outage probability and ergodic secrecy capacity were derived.

Khandaker *et al*. in [140] propose a truth-telling based mechanism, where the relays are forced to tell the truth, otherwise they are penalized; which is also called incentive control mechanism. The relay is selected from a group of relays interested in gaining the incentive. The incentive of energy harvesting from the signal causes the relays to allure to transmit the message. The authors also provide performance comparison of incentive control mechanism with another power optimization algorithm.

The secrecy performance for an uplink scenario, where a relay is equipped with multiple antennas in SIMO mixed RF/FSO system, was studied in [141]. More specifically, the impact of maximum ratio combining (MRC) or selection combining (SC) on the secrecy performance was evaluated when the relay combine received signal at different antennas. Of late, multiuser and multirelay selection strategies are proposed by the authors in [142], [143]. The relays are considered to be able to perfectly decode information and transfer it to BS, in the presence of an eavesdropper.

Shim *et al*. in [144] consider a generalized scenario in a multirelay network where a cluster of M sources transmit messages to a cluster of N relays, in the presence of a single eavesdropper and a single destination. The eavesdropper is assumed to utilize either MRC or SC to combine the signal during source-to-relay and relay-to-destination transmission phases. It has been deduced that increasing number of relays has more impact than increasing number of sources.

Confidential transmission of messages for bidirectional communication was studied in [145]. A DF relay is used and strong secrecy capacity regions are established. It was demonstrated that a conventionally used weak secrecy capacity region coincides with a strong secrecy capacity region. The authors proposed an optimal relay selection scheme for AF, and DF relaying in [41] for a given eavesdropper. Bao *et al*. in [146] extended the system model by introducing multiple eavesdroppers in the presence of multiple relays. The authors proposed three different relay selection protocols to exploit the diversity gains obtained using multiple relays. Afterwards, Yang *et al*., in [147], evaluated the secrecy performance of a downlink single BS, single DF relay and multiple destination environments. The authors considered switch-and-stay combining scheme to improve the battery lifetime and scheduling complexity, while using antenna selection scheme to reduce leakage of information. The MRC was used to combine the messages when CSI of the eavesdropper is not available. The authors in [42] investigated the secrecy performance for large scale MIMO relaying systems when the CSI of wiretap channel is not available, and the CSI of the main link is imperfect.

3) Relay Ordering: The authors in [148] proposed a strategy based on the work of [149], [150], where the relays are ordered according to their distance from the transmitter. To be more precise, the closest DF relay decodes its message first and then forwards it to the next relay. The same procedure

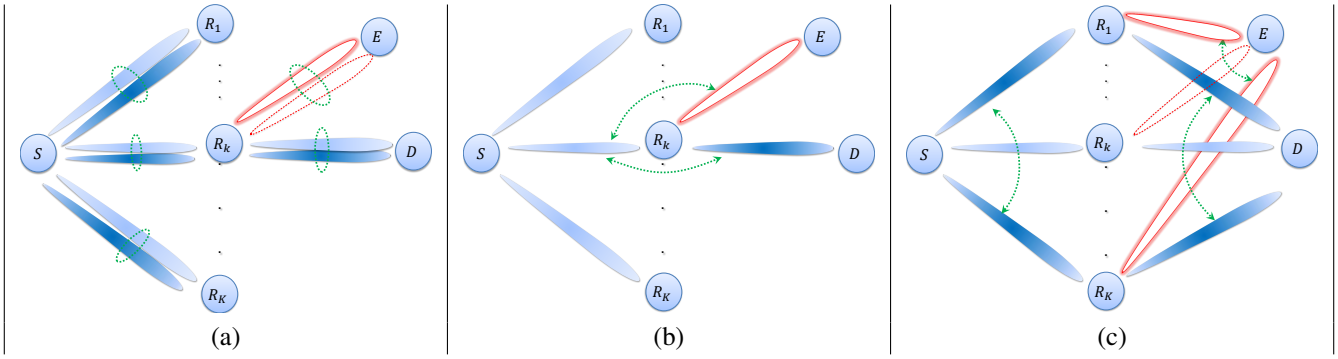


Fig. 9: Different channel correlation conditions (a) Correlation between the actual and the corresponding estimated channels (b) Correlation between source-relay and relay-destination links of same relay (c) Correlation among source-relay links and among relay-destination links.

occurs in a multi-hop fashion until the message reaches the destination. The authors first studied the secrecy performance in a single relay environment. They considered DF-based cooperation in a multi-relay network and proposed three different strategies based on ZF, as shown in Figure 10. In multi-relay single-hop schemes, the relays that receive the message from S directly forward it to D through cooperative beamforming. However, for K-hop and $K/2$-hop strategies, the transmission takes place in multiple hops. Particularly, in the K-hop strategy, the first relay R_1 forwards the received message to R_2 and D while R_2 forwards the same to R_3 and D, and so on. In contrast to single-hop communications, the K-hop scheme uses the partial ZF technique. In $K/2$-hop strategy, it was assumed that the total number of relays is even, and thus, these relays can be divided into $K/2$ clusters. In each cluster, there are two relays, wherein, the signal received by R_1 and R_2 in the first cluster is forwarded to R_3 and R_4 in the second cluster, and so on. The authors also proposed a suboptimal scheme for power control. Their results showed that it is disadvantageous to enable only partial ZF in every transmission block.

In a similar work [18], authors analyzed two ordering policies with TAS. The closed-form expressions were derived for outage probability of the secrecy capacity, for each ordering scheme. The results reveal that TAS improves the secrecy rate, as compared to single-antenna systems, yet the TAS increases with the path loss exponent. Moreover, the impact of the ordering policy reduces for higher path loss environments.

C. Unique Challenges of Secure Cooperative Relaying

Some challenges related to cooperative relaying are illustrated in Figure 11.

1) Determination of Trustworthiness: Trust in communication network is generally defined by a particular metric. The degree of trust, in general, is the level of belief that one node has for another node for a specific action [151]. This degree of trust usually depends on the amount of available information (direct or indirect) from previous observations [152]. For instance, node j receives information that a node k usually transmits its messages. This type of information is direct, however, if the same information is received from any other node then it becomes indirect. This methodology has critical inherent flaws from a secrecy point of view. First of all, a relay can perform bad mouthing or broadcast false information [153]. Secondly, a relay can display conflicting behaviors, like behaving differently for a particular node or group of nodes. Doing so will result in gaining trust of some nodes while it will become untrustworthy for other ones. Hence, a clear demarcation between relays, in terms of their trustworthiness, is imperative because an untrustworthy relay introduces uncertainty, whether a relay is an eavesdropper or a helper.

2) Position of Relay: Mobile networks face different challenges, as compared to static networks, when it comes to provisioning of link security. The following two reasons are explaining why:

1) The vehicles' high speed results in rapid changes in channel coefficients [154], [155], [156], [157].
2) The position of a source, relay and destination quickly changes, resulting in the issue of nodes authentication.

The above-mentioned issues can be addressed by using robust CSI evaluation strategies, as CSI is the most important component of PLS. In addition to this, adaptive security protocols may be provided, along with the inclusion of the upper layers to provide security in cooperative networks. Also, the position of the relay in a mobile networks is a potential method to utilize mobility. The position of mobile relay, with respect to the position of the source, destination and eavesdropper, is significantly important to ensure information theoretic security. Traditional approaches consider the role of relays based on their position [158], [159], [143]. Particularly, the relays near the source are used to relay information to improve the SNR at the receiver. However, one major drawback of this approach is the assumption of fixed locations of the sources and eavesdroppers i.e., the legitimate users and eavesdroppers need not to be static at any particular position. This may also result in pilferage of information where relays are deployed as static entities. One possible solution is in the form of deployment of mobile relays [160], [161], [162], [163]. In this context, the mobile relays can improve the secrecy by using the flexibility to move in the network. Some of the major issues with this approach are 1) the mobile relays should be aware of the number of eavesdroppers and their position, 2) signaling overhead can significantly increase in order to ensure

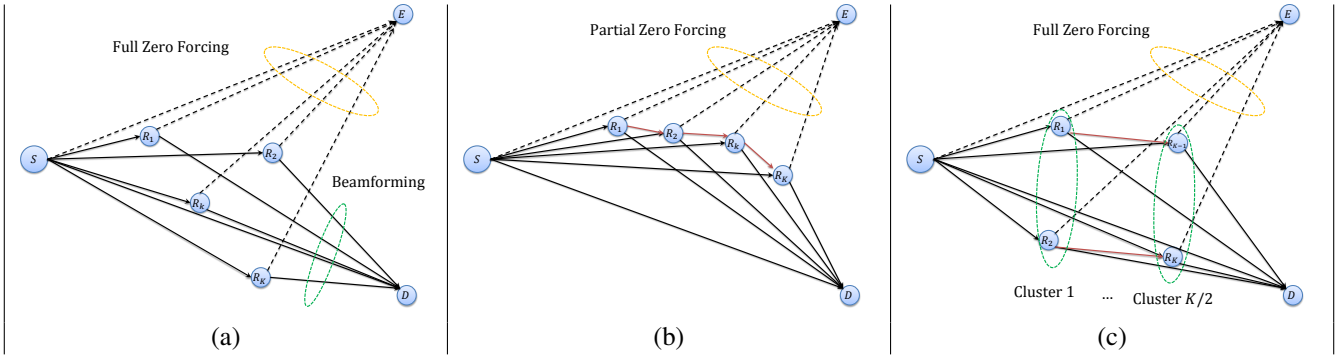


Fig. 10: (a) Multiple relay single-hop strategy (b) Multiple relay K-hop strategy. (c) Multiple relay ($K/2$)-hop strategy.

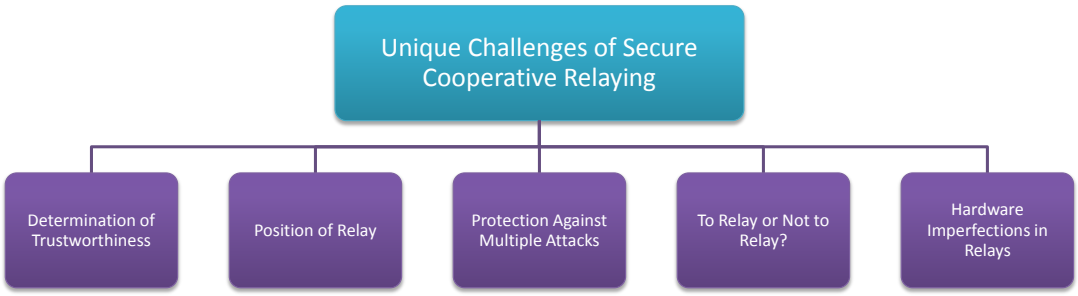


Fig. 11: Open issues in secure cooperative relaying.

cooperation among relays.

3) Protection Against Multiple Attacks: Many studies on PLS address either passive or active eavesdroppers. In case of passive eavesdroppers, the defending can be ensured using cooperative techniques. However, the case where both passive and active eavesdroppers are present in the network has not been investigated extensively. There is a need to ensure the security using cooperative communication, when the passive eavesdropper tries to listen to the transmission, while the active eavesdropper tries to jam the transmission between legitimate users. In this context, design of flexible cooperative protocols for providing link security is considered necessary.

4) To Relay or Not to Relay?: Although there is a number of advantages of using relays, yet there is an associated drawback of relaying techniques that cannot be neglected. The needed additional overhead, for secure cooperative relaying, needs to be quantified. The user should be aware of the achievable rate of transmission and associated delays and probing overheads prior initiation of communication. Intuitively speaking, the tradeoff between secure throughput, delay and signaling overhead should be well established to make the communication secure and worthwhile. A study that partly answer this question was performed by Gong *et al.* in [164], however, a fixed number of relays in the network was considered. A secure relay selection and tradeoff evaluation, in the presence of different numbers of relays at different times, is yet to be explored.

5) Hardware Imperfections in Relays: Imperfect response of hardware in the form of phase noise, imbalances in inphase and quadrature phase and non-linear power amplification can severely degrade the performance of relays. Only a handful of studies have considered secure cooperative relaying [165], [166], [167], [168]. Although these studies have remarkable impact in PLS literature, yet they separately consider the said impairments. Moreover, these studies are limited to the study of a single cell, and under perfect channel estimation. It is also necessary to further investigate the joint impact of these hardware impairments on the secrecy performance of networks.

IV. Cooperative Jamming for Security

The importance of AN in the area of PLS is enormous. In fact, if it is added in a controlled manner, it can make the whole difference between the way signal is interpreted at the legitimate receiver and at the eavesdropper. The magnitude of AN that adds to the signal is therefore an important concern. It may be noted that in an ideal case, the power to transmit signals should be minimized, however, in order to secure the message, additional power is added in the form of AN. This asks for algorithms to be developed for optimum power allocation.

AN is an enabler of cooperative jamming (CJ) techniques. Jamming at the eavesdropper is generally performed using one or more of the techniques shown in Figure 12. In particular, Figure 12 (a) shows the case where a dedicated jammer J is employed to interfere with the eavesdropper's received signal. Since the dedicated jammer may not be a part of the legitimate transmission, the interference signal can also be received at D thus degrading the secrecy performance of the system. However, some incentivized game-theoretic techniques with appropriate power allocation policies, also discussed later, can be used to improve the secrecy performance. In case a dedicated helper node is not available, then it is up to S

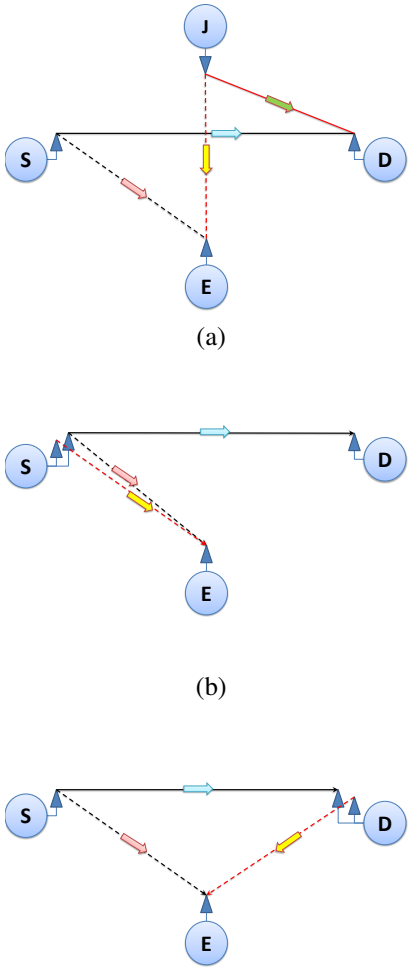


Fig. 12: Different jamming conditions (a) Helper node assisted (friendly) jamming (b) Source assisted jamming (c) Destination assisted jamming.

or D to degrade the signal reception of the eavesdropper. Typically, this can be accomplished if either S or D is equipped with multiple antennas as depicted in Figures 12 (b) & (c), respectively. Note that both S and D should secretly exchange jamming information in advance to avoid degradation of their secret communication. It is also worth mentioning that both S and D can be equipped with multiple antennas to simultaneously jam the reception of the eavesdropper, though for the sake of simplicity, we have only focused on minimal jamming requirements at S and D. Orthogonal jamming can be combined with AN to provide better secrecy performance [169]. This study proved that the secrecy rate can be increased and the SOP can be reduced by using orthogonal jamming, as compared to the secrecy performance of only AN. CJ is suited when the eavesdropper has a single antenna. However, if the eavesdropper is equipped with multiple antennas, CJ may not work efficiently. This is one of the fundamental problems with jamming techniques: an eavesdropper with multiple antennas can use beamforming to cancel interference and get better signal-to-interference-and-noise ratio (SINR). A brief summary of recently proposed CJ techniques, for the case of both single and multiple eavesdroppers is provided in Table VI.

A. Jammer Power Allocation

Power allocation between main signal and friendly jamming signal is one of the key criteria to increase the secrecy in CJ systems. In general, the optimal power allocation depends on following two conditions:

1) Availability of the global CSI of the network entities at the source's side.
2) Availability of the neither statistical nor instantaneous CSIs of the eavesdropper.

If the available power is P_{max} and transmit power is P_t, then a typical power optimization for maximization of achievable secrecy rate C_{sec}, can be formulated as

$$\max_{P_t<P_{max}} C_{sec}, \tag{14}$$

In regards to above-displayed equation, following salient details can be provided

- The optimal solution relies on the availability of global CSI and the solution is typically traceable in quasi-static fading.
- The instantaneous solution is not traceable when only statistical CSI is available [170]. In that case, Jensen equity and specific bounds on the ergodic capacity can be exploited for optimal power allocation.
- A variety of factors also affect the optimal power allocation including spatial location of legitimate nodes and eavesdroppers, and available maximum power.

Tang *et al*. in [171] focused on secure downlink in multiuser scenarios and derived the closed-form expression for optimum power when the transmitter has multiple antennas. The eavesdropper acts passively and the users, as well as eavesdroppers, have perfect knowledge of CSI. Three precoding techniques were provided i.e., channel inversion (CI), zero forcing (ZF) and regularize channel inversion (RCI). The authors noted that RCI performs better than the other two precoding techniques. It has been learned that the secrecy rate decreases with N and alpha.

The CSI, as discussed before, is very important for secure data communication. If the CSI of the eavesdropper is not known then beamforming can be done to retain security. In general, the CSI of passive eavesdropper is not perfectly known. Li *et al*. verified that AN aided beamforming, as shown in Figure 13, can considerably improve the secrecy capacity [172]. The same authors provided two solutions namely, deterministic uncertainty model (DUM) and stochastic uncertainty model (SUM). For deterministic case, a semi-definite solution is proposed and for stochastic case, a suboptimal solution is provided. The authors solve the worst case secrecy rate maximization (WC-SRM) for DUM and outage probability based secrecy rate maximization (OP-SRM) for SUM. The DUM model quantizes the CSI at receiver and send it back and SUM assume the error to be Gaussian distributed. The DUM has been investigated in literature before as well but without

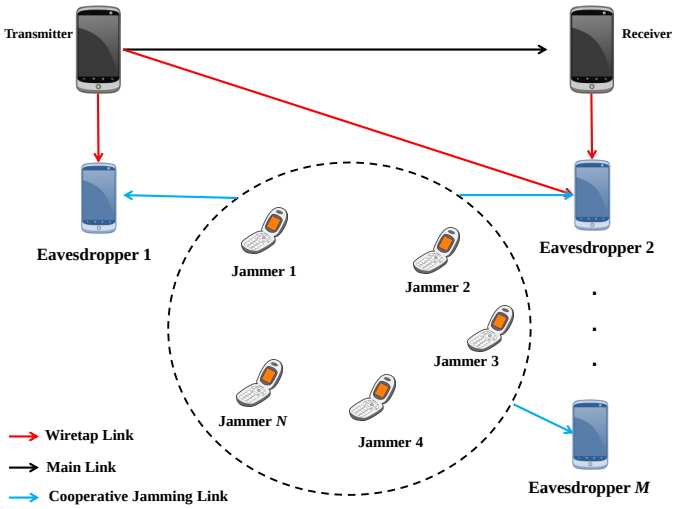


Fig. 13: CJ using multiple jammers.

AN. By combining AN and DUM, the performance of secrecy rate improved far above the case which only considered DUM on the main channel. Similarly, the secrecy rate decreases for SUM case as the variance increases.

Optimum power allocation for AN secure MIMO precoding system is considered in [173]. The authors derived a closed-form expression for power allocation to maximize secrecy rate and it has been concluded that the tightness of the derived bounds depends upon the number of transmit antennas. AN is used to degrade the eavesdropper channel, the scheme also called "mask beamforming" or "mask precoding" in MIMO channels. AN precoding divides the total power P between noise and information signal. AN precoding ensures a positive secrecy rate even if eavesdropper noise variance approaches zero. The simulation result shows that as the number of transmit antennas increases, the secrecy rate increases as well.

AN-aided secure multi-antenna transmission scheme with limited feedback, was provided in [174]. In particular, a multi antenna scenario is considered with AN added beamforming plus feedback from a receive antenna. Again the focus is on the connection outage constraint of the main link and secrecy outage constraint of the eavesdropping link. An adaptive scheme for coding parameters and power allocation between AN and message data is considered. Recent work relaxes the requirement of CSI for the transmitter and allows a fraction of error to be added in the actual CSI. These models may not be good for limited feedback channels due to oversimplification of real-world problems in order to know the exact number of errors in the estimated CSI. Therefore, the same authors use limited feedback so that AN may leak into the desired channel. A rate-adaptive transmission technique has been given to cope with the leakage of AN. Specifically, if the feedback bits are significant in amount, then more power is allocated to the data and less power to AN.

Power-constrained optimal CJ for multiuser broadcast channel is introduced to maximize the secrecy of the network in [175]. Optimal CJ is done with friendly jammers to provide PLS. Here, the authors derive a lower bound for eavesdroppers SNR and extend asymptotic secrecy rate. The most recent approach of CJ is that the source transmits data to a legitimate receiver in presence of eavesdroppers. In their work, the source, the jammer, and the legitimate receivers are assumed to have N, L, K antennas, receptively, and the single eavesdropper has M antennas. The authors noted that for $L-K<M$, even with the inclusion of friendly jammers, the secure communication is not possible. The simulation results show that by increasing the transmit power at BS, the maximum SNR of the eavesdropper can be significantly reduced.

In [176], the authors used game theory to investigate the interaction between the source and the friendly jammers. Specifically, the source must pay friendly jammers to interfere with the eavesdropper reception. The authors investigated the price-performance trade-off and concluded that if the price set by the jammer is low, then the profit to the jammer would be low as well. However, if the price set by the jammer is too high, then the source may not buy at all. In addition, the authors also showed that centralized and distributed jamming schemes have a similar performance when gain per unit capacity is significantly larger.

In [177], the authors proposed a cooperative jamming approach by using a Stackelberg game in which the primary users act as leaders and the secondary users constitute the followers. Their proposed framework allows secondary users to transmit jamming signals with pre-specified probabilities and both the primary and secondary users are able to access the same channel in order to minimize the spectrum holes for secondary access. The evolutionary behavior of the system was modeled by a Markov chain and the Stackelberg equilibrium solutions were derived. However, the authors did not consider user fairness, which would require system modeling with a complex Markov chain.

B. Beamforming Approach

Among the techniques studied so far, cooperative beamforming (CB) is one of the important ones. This technique is particularly important when there is no direct link from the transmitter. A study of the CB for DF relay has been already conducted. For AF, the beamforming technique is difficult because of the noise amplification, however, techniques like CB and CJ come into play when there is a direct link from the source to relay, and the nodes are only performing the jamming. Null space technique is used to nullify the AN at the receiver.

The AN can be combined with several other techniques to further enhance secrecy of information. One technique is to combine AN with CB [178]. The goal is to optimize AF matrix and AN covariance for secrecy rate maximization. Polynomial time optimization technique is proposed, based on two level optimization and semi-definite relaxation (SDR).

Secrecy rate maximization problem is presented in AN-aided beamforming for multiple-input single-output (MISO) wiretap channels [179]. The authors assume that the CSI of the legitimate channel is perfectly known, while the eavesdropper is a Gaussian random vector. The complete solution

for secrecy rate maximization (SRM) with optimal power allocation is provided, while keeping in view the outage probability constraints. AN can more effectively outperform an eavesdropper since it encounters every interceptor (both passive and active). Moreover AN can be generated knowing only main channel. Previous solutions to the said problem are suboptimal. Sometimes AN may be injected in the main channel, if the channel is fast fading to increase ergodic secrecy. AN-aided beamforming technique can be used to increase secrecy performance in faded channels, significantly improving the the secrecy rate.

If the channel between the transmitter and the receiver is weaker than the transmitter and the eavesdropper, then secrecy rate is almost 0 and using single antenna may not be a good approach. Therefore, the authors in [180] take the advantage of weighted optimization, with the goal to assign the optimal weights to antennas and optimal power to wireless nodes. The authors consider a single transmitter, a trusted relay, an eavesdropper and a receiver. The source transmits the message signal and the relay transmits the weighted version of it. In the presence of an eavesdropper, the secrecy rate is the figure of merit and it depends upon the difference of the secrecy capacities of the main and wiretap channel. Secrecy rate increases with the increasing number of antennas, and transmit power gets reduced. Intermediate nodes perform the function of adaptive beamforming as well as CJ.

The authors of [181] considered a network of multi-antenna legitimate and eavesdropper nodes and they proposed an optimal transmission strategy for this MIMO wiretap channel. The authors considered that the instantaneous CSI of the eavesdroppers was known at the transmitter, which could then perform power allocation between data transfer and broadcasting an interference signal. The authors modeled the interaction between the transmitter and jammer as a two-person zero-sum game and also considered the scenario where the players move sequentially under imperfect and perfect knowledge of their opponents' response. The authors demonstrated that changing a single parameter can significantly change the outcome of the Nash equilibrium.

In [182], Chu *et al*. formulated a secrecy rate optimization problem in the presence of cooperative jammers and multi-antenna eavesdropper. The authors divided the convex optimization problem into two sub-problems: In the first problem the transmit covariance matrix was optimized, while in the second problem the covariance matrix of the cooperative jammers was optimized. Subsequently, it was proven that the revenue functions of transmitter and cooperative jammers are concave. The authors used a Stackelberg game to maximize the secrecy rate and provided the Stackelberg equilibria for the said game.

A virtual beamforming based jamming technique was proposed in [183]. The authors modeled the relationship between cooperative jammers and the source node by using a Stackelberg game in which the source paid cooperative jammers to transmit interference to the eavesdroppers. The jammers competed with each other to provide a reasonable price and the same was modeled as a non-cooperative game. By assuming a constant security rate between the source and the destination node, the equilibrium point for the pricing strategy was derived. Furthermore, a joint optimization strategy for power allocation and power pricing was derived. The authors showed that the power pricing and power allocation games converge to a single optimization point.

C. Jamming with Secure Key Exchange

In [184], the authors highlighted the limitation of traditional key exchange mechanisms in the application layer of OSI. These mechanisms are affected and overloaded by processing and needed a trusted mediator. Due to eventual growth complexity, the prescribed techniques started showing poor performances. To minimize this effect, the authors proposed a novel key substitution technique in Physical layer, which is based on the concept of self-jamming and exploits the features of OFDM. Their system model consisted of passive adversary between two legitimate users (transmitter and receiver) in FD mode. For the receiver FD mode served the purpose to act as both signal receptor and jamming node. It compensated the shortcomings of application layer secret key production/ exchange techniques. Their simulations conclusively illustrated that a private key could be exchanged safely between transceivers at a considerably less BER despite the existence of an adversary. The simulation depicted the results that an adversary had to randomly guess an exact key, with an increase in the BER of eavesdropper. In other words, multiple trials had to be performed by an adversary in order to guess an exact key.

The authors in [185] emphasized the privacy of a PLS technique using an induced artificial interference to obliterate the substitution of a secret key, allowing the receiver to sabotage random chunks of propagated signal. The authors increased the eavesdropping capabilities of the adversary by fortifying the eavesdropper, and then placed several antennas on the eavesdropper's side. Moreover, the interference of the jamming signal with the useful signal depends on the positions of the receiving antennas, considering multipath propagation. In this context, they designed an algorithm to distinguish between normal and jammed signal parts to unveil the transmitted signal. To validate their findings, their methods included simulations and practical experiments, using software-defined radio environment and utilized the wireless open-access research platform (WARP). They demonstrated that in the OFDM based multiple antenna system, adversary/eavesdroppers easily decreased the privacy during the key exchange and easily transcends single-antenna ones.

D. Protected Zone Approach

We may sometimes be interested in providing security to a particular location, the intended receiver may even sometimes be located in a particular location. Therefore, instead of providing security in the entire area, we may be interested in providing security in a section of that area instead. AN can be used to ensure protected zones [186]. The secrecy zone is defined based on transmission power and stochastic approach, to provide secrecy to target zones. The authors deploy a protected zone around the transmitter, and for this

protected zone, the radius is the parameter to be optimized. The assumption here is that the transmitter has multiple antennas and both the receiver and the eavesdropper have a single antenna.

The case where AN was generated by the intended receiver, was considered in [187]. This approach removes the need for CSI feedback, and there is no need for the number of eavesdropper antennas to be smaller than the number of legitimate receivers. A geometric secrecy concept was introduced so a given geographical region can be protected. If the eavesdropper is passive, then a probabilistic model will be used for CSI and the secrecy outage region can be defined. The SOP changes with the movement of the eavesdropper, wherein, as an eavesdropper moves closer to transmitter, the outage increases and decrease as it gets closer to the receiver.

A protected zone is an area free from any eavesdropper and only have trusted relays. The authors define a protected zone close to the transmitter and if any eavesdropper comes close, a high-level security will then be needed. A weighted normalized cost function (WNCF) is considered for an optimal power allocation and radius of protected zone. As demonstrated, increasing the power for the signal alone may not be that benefiting, an optimal method of power distribution between the information signal and AN is then needed. The size of protected zone decreases with power, and for a high target secrecy and minimum power, the size of the protected zone reaches its max. The power reaches a state where no more power is needed to increase the secrecy.

On the other hand, AN can be used to perform authentication thus enhancing PLS [188]. The CSI of the legitimate user is employed for authentication purpose, which obviously differs from the eavesdroppers' CSI. AN will be added to the received signal to enhance security performance in time variant channels. The probabilities of miss-detection and false alarm as a function of doppler spread were studied. As the doppler spread increases, both probabilities increase, showing the negative effect of channel variability on the secrecy performance.

Nabil *et al*. in [189] investigated a novel transmission scheme by incorporating the known location of the eavesdropper. They also assumed that the transmitter has incomplete information of the channel state of the legitimate receiver. The authors also defined protected zones to provide spatial secrecy against the eavesdropping attacks. The security is improved by allocating optimal transmission power, and by varying the size of the protected zone. The authors finally quantified the required amount of power for preventing the eavesdropping attack in closing quarters.

The authors in [190], similar to protected zones, introduced the concept of guard zones and a comparative analysis of guard zones were provided with the AN. In particular, the authors derived the closed-form expression of the threshold on the density of the eavesdroppers, for both guard zone and AN techniques. This helped to characterize the fact that the guard zone technique performs better when the distance between the legitimate users is greater than the threshold, as earlier derived by the authors.

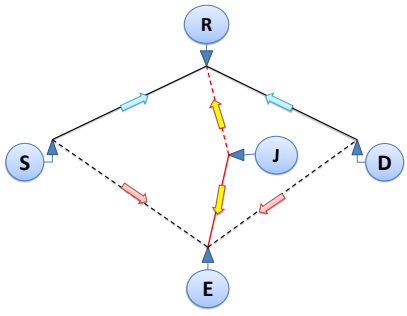
E. Partial Jamming

Partial jamming is an emerging paradigm for the design of efficient jamming strategies. It works on the assumption that an eavesdropping node is not capable of deciphering the secret message by decoding only a part of the transmitted signal. More specifically, a friendly jammer transmits an interference signal in specific time slots to prevent the eavesdropper from receiving the complete signal [191]. Thus, the eavesdropper may not acquire the complete information due to receiving jamming signals in certain time slots. Note that the partial jamming technique is different from the aforementioned jamming designs that perform jamming for the entire communication duration and it is also different from the partial jammer selection techniques [192], [193], [194], [195] that select jammers based on the availability of partial CSI for the main or the wiretap links.

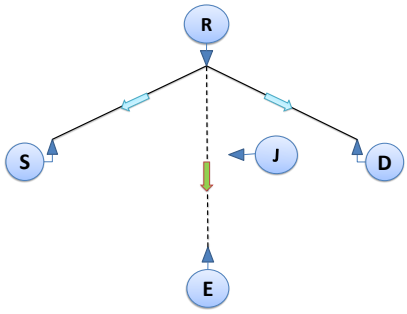
Figure 14 shows the partial jamming operation in a two-way relaying scheme. The figure shows that communication takes place in two time slots: during the first time slot, both legitimate nodes S and SD transmit their messages to the relay R while the jammer J broadcasts its signal to R and E. However, R can remove the jamming signal before message decoding as it has a priori knowledge of the jamming signal. During the second time slot, as shown in Figure 14 (b), J refrains from jamming to conserve its power while R broadcasts its received superimposed signals of S and D. Since S and D already know their own messages transmitted during the first time slot, these can be easily removed from the composite signal received at S and D. In contrast, E may find it difficult to decode the message of either S or D due to its receiving only partial information during the first time slot.

Since partial jamming is a relatively new concept, limited work has been done so far to investigate its secrecy performance. In [196], the authors proposed to combine watermarking techniques with the iJAM jamming mechanism [197]. According to the iJAM design, the legitimate transmitter broadcasts its message twice and the legitimate receiver randomly jams the broadcast message. In this way, only the legitimate receiver knows which of its symbols were jammed and can discard them, whereas the eavesdropper remains oblivious of this information. The authors noted that an eavesdropper requires phase correction information between sender and receiver to completely decode the symbols. Moreover, they showed that a larger secrecy capacity can be achieved with their proposed design when compared with another benchmarking protocol namely watermark-based blind physical layer security (WBPLSec) protocol.

More recently, Chensi *et al*. analyzed partial jamming in the worst-case scenario that the eavesdroppers' CSI is not available at the legitimate nodes and that the eavesdroppers' node density is larger than the density of the helper nodes [198]. The authors concluded that the jamming should be performed during the first time slot as the information leakage is more dominant during this time slot; while the signals are overlapped during second time slot. The authors also showed that the single-time-slot jamming is more power-



(a)



(b)

Fig. 14: Partial jamming (a) First time slot (b) Second time slot.

efficient than the dual-time-slot jamming. Their complexity analysis of partial jamming techniques showed that the number of floating point operations required for partial jamming is less than that required for full jamming.

It can be deduced from the aforementioned discussion that partial jamming is suitable for power-constrained systems. However, more research efforts are required to address design issues such as how to minimize the impact of the jamming signal on the legitimate receiver, when to send the jamming signal and how to deal with the diversity/ cooperation of eavesdroppers.

F. Exploitation of Cross-Layer Opportunities

One promising technique, to improve security in cooperative networks, is using cross-layer approaches. The deployment of the authentication, at different layers, can potentially increase the security in cooperative networks. However, due to this cross-layered security, the feedback overhead and complexity of hardware can considerably increase. Consequently, it is necessary that the tradeoff between complexity and security be well defined. The authors in [199] highlighted all of the aspects of the PLS schemes with respect to space, time and frequency domain. Since the wireless networks are not secure enough for a reliable transmission of the data, the authors focused on highlighting threats and attacks including tampering, leakage of private information, interference from unintended users, network flooding, jamming and eavesdropping. The techniques suggested to solve these security issues are the Yarg code and amplify and forward compressed sensing (AF-CS) method.

The alignment of sub-messages can be helpful in increasing the secrecy of information. In this secrecy enhancement technique, the transmitter divides the message into M sub-messages. Each helper also sends a jamming signal to confuse the eavesdropper. The M sub-messages can be separated at the legitimate receiver, due to their irregularities. Also, each CJ signal is aligned with the message signal. This alignment ensures that the information leakage to the eavesdropper is minimum. Hence, each message signal is protected at the eavesdropper by one of jamming signal. However, this scheme requires the CSI of the eavesdropper and legitimate link to align the message and jamming signal [200], [201].

The problems of analyzing the characteristics of signals and random processes may be solved by probabilistic approaches. A stochastic approach may very well be applied to the situation involving PLS [202]. The BS is Poisson distributed, whereas, legitimate and eavesdropping nodes are assumed to be randomly distributed. The authors assume a downlink scenario and an orthogonal multiple access technique. Many BS are intended receivers while others are eavesdroppers. The secrecy rate here depends on the eavesdroppers density, and as the eavesdropper's density decreases, the secrecy capacity significantly increases.

If the legitimate receiver has more antennas, the results are then even more valuable. In this case, the signal reception of eavesdropper can be jammed using a special noised called PDF-band-limited [203]. The focus of earlier studies is mostly on an asymptotic approach, whereas in this work, the eavesdropper's reception is jammed using a special noise. As long as the main channel is better than wiretap channel, positive secrecy rate can be maintained but does not guarantee perfect secrecy, as per Shannon criteria. The characteristics of additive noise matters, therefore, band-limited additive noise was considered by the authors. This is different from Gaussian channel and provides possibilities for designing such encoders which can improve the secrecy of transmitted information. AN is sent intentionally by a legitimate part which gets added with AWGN noise of channels, and an overall noise is received by both legitimate receiver and eavesdropper. It was found that with the selection of a *proper jamming distribution*, secrecy can be significantly enhanced.

A joint physical and application layer security scheme is considered for provisioning of security in [204] where signal processing is employed at physical layer and authentication, and watermarking at the application layer, as shown in Figure 15. It is mainly because the PLS measures neglect the application layer security measures and vice versa. A cross layer security measure will be a best solution to jointly cope with the issue of security. In PLS, the focus is mainly on the secrecy rate and the CSI is generally needed to calculate the secrecy rate. Since the full CSI is generally not available, therefore, a quasi-static fading channel is assumed in most of the work. Another technique is information processing approach (IPA) where different kinds of noises and signals are added to confuse the eavesdropper and enhancement of secrecy rate. Two main tasks are performed on the application layer authentication:

1) Who transmits the message? (Identification)
2) Whether the transmitted message has been altered or not? (Authentication)

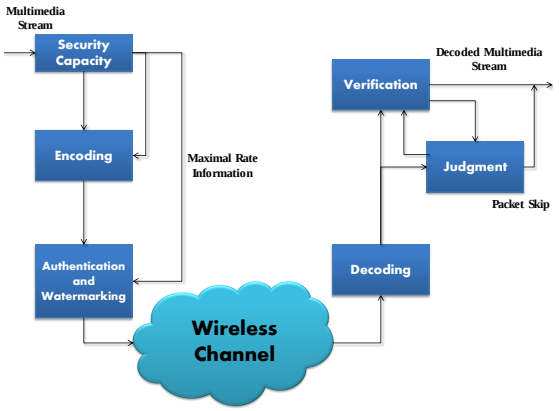


Fig. 15: Joint physical-application layer security scheme [204].

In another work, joint channel characteristics for PLS technique were investigated [205]. The problem of untrusted relays is considered, and joint channel characteristic, i.e., source-to-relay and relay-to-destination, is exploited. The AN is then added, and both internal and external eavesdroppers are dealt with. Also optimal power transmission is taken into consideration that combines both the source-to-relay and relay-to-destination channels and extract the joint channel characteristics. It then adds AN and calculates the secrecy capacity and optimum signal power. Again the transmitter is a multi antenna device and relays are multiple with single antennas. The message is first encoded to Gaussian random variable, and the symbols are further processed by a matrix. Channels are considered flat fading. Relays are assumed to be operated on AF protocol and CSI is assumed to be known globally, by the authors. Simulation results show that secrecy rate is improved when the AN is in the null space of legitimate receiver.

G. Unique Challenges of Secure Cooperative Jamming

We now highlight some of the particular challenges of cooperative jamming to enhance PLS, as given in Figure 16.

1) Incentive Based Jamming: Although several studies have investigated cooperative jamming [230], [210], [231], [194], [232] and destination assisted jamming [233], these studies consider that the jammers (helper nodes) in the network are generous enough to provide their services without any incentive. Generally, any dedicated helper node in the network is difficult to realize, as nodes tend to make independent and selfish decisions in large scale networks. Game theoretic approaches can be used to partly understand this interaction [176], [234], [235], [182], [236]. It is pertinent to mention that even these studied do not consider real-time fluctuations of locations of nodes, and suboptimal precoder assumption based results are obtained. Thus, the study of complex interaction between jammers and other network entities and parameters is still an open issue, and should be the focus of future research work.

2) Cooperative Jamming under Correlated Channels: It has been commonly observed that the fading conditions, due to less separation between the two nodes in space or time domain, are quite similar [237], [238]. Most of the studies on PLS assume the channel between jammer and destination, and that between jammer and eavesdropper, to be independently distributed. This is an oversimplification; it may not be true for most of the cooperative scenarios. It is because the fading correlation has a significant impact on the fading correlation [239], [240]. In addition, the system performance, under correlated fading for multiple antenna jammer, can notably vary from the case where independent fading is assumed. It is therefore essential to quantify the performance tradeoffs under correlated fading.

3) Inaccurate Power Allocation under Imperfect/ Unavailability of CSI: It has been stated previously that the availability of CSI for all nodes across the network, including the eavesdroppers, results in the maximum secrecy rate. But in practice, the legitimate nodes may only have limited or no access to the CSI at the eavesdropper, especially if the latter operates in passive mode. This issue is more concerning for jamming nodes because power allocation schemes for cooperative jamming usually depend on a perfect channel estimation. For instance, the CSI of the legitimate user is usually obtained by feedback. A handful of studies under jamming have evaluated the secrecy performance of under imperfect channel estimation for imperfect legitimate channel [241] and for main and jamming links [242], [182], [243]. In addition, these works derive lower or upper bounds, and closed-form expressions for aforementioned scenarios are largely missing in the literature. Moreover, during feedback transmission from the legitimate user, the eavesdropper can also get the information and use it to adopt a more destructive interception strategy. It is therefore necessary to further investigate the impact of channel estimation errors, especially for the case of colluding eavesdroppers and to design optimal and secure CSI feedback mechanisms.

4) Standardization of Cooperative Jamming: In order to minimize the gap between research efforts and practical implementation of the device cooperation, standardization is necessary. It is considerably difficult to standardize the friendly jamming, under different network topologies, because of decision based nature of jammers to either cooperate or stay independent. For instance, a node a can cooperate with source node s to jam the signal of node x (a potential eavesdropper for s) for a particular time. After some time, it is possible that node a wants to send a message to node x (being part of the same network). In this simple scenario, how should node x react to the request of a, given the fact that a tried to send jamming signals few moments ago. Conditions like this demand a dynamic standard for cooperative jamming, which is still nonexistent partly owing to the novelty of cooperative jamming strategies. Therefore, it is one of the important directions to conduct future research work.

5) Cooperative Jamming under Multi-cell Environments: There is no denying the fact that notable strides have been made to improve the link security using above-mentioned cooperative jamming technique, yet large part of this work, is limited to a single cell environment only. The extension of these jamming schemes for a multicellular environment can reveal many deficiencies in them, e.g., it is more difficult

TABLE VI: Overview of recent advances in cooperative jamming.

Eavesdropper(s)	Reference(s)	Single Jamming Node	Multiple Jamming Nodes	Destination Assisted Jamming	Solution
Single	[122]	-	-	✓	Proposed a novel design for optimal jamming covariance matrix to maximize the secrecy rate and mitigates loop interference associated with the FD operation.
	[206]	-	✓	✓	Proposed an efficient suboptimal algorithm for the majorization of system parameters to avoid global search and the practical case without availability of eavesdroppers' CSI.
	[207]	-	-	✓	Proposed an optimal power allocation algorithm for jamming noise.
	[208]	-	-	✓	Proposed a transmission scheme, by maintain a scaling law of the achievable secrecy rate, to maximize the secrecy performance.
	[209]	-	-	✓	Proposed a power allocation scheme by considering imperfect CSI of nodes, to maximize the secrecy rate.
	[210]	-	✓	-	Proposed an optimal jamming noise structure under global CSI in which secrecy rate performance is improved very close to the optimal one.
	[211]	-	✓	-	Derivation of the optimal source covariance matrix to maximizes the secrecy rate subject to probability of outage and power constraint.
	[212]	✓	-	-	Derivation of new tight-closed-form expressions of the ergodic achievable secrecy rate for three secure transmission schemes i.e. (1) artificial noise aided precoding (ANP), (2) destination based jamming (DBJ) and (3) eigen-beamforming (EB).
	[213]	-	✓	-	Derivation of closed-form expressions for the optimal weights and power allocation to maximize the difference in the SNR between destination and eavesdropper.
	[214]	✓	-	-	Proposed a distributed mechanism to develop jamming participation algorithm by compensating non-cooperative nodes with an opportunity to use the fraction of legitimate parties' spectrum for their own data traffic.
	[169]	✓	-	-	Proposed a novel CJ method to prevent eavesdroppers from using beamformers to suppress the jamming signals.
	[215]	-	-	✓	Proposed a destination-assisted jamming and beamforming (DAJB) scheme to improve PLS. Also presented optimal power allocation algorithm by solving the second-order convex cone programming (SOCP) together with a linear programming (LP) problem.
	[216]	-	✓	✓	Proposed optimal and suboptimal power allocation schemes for maximizing achievable secrecy rate subject to a total power constraint.
	[217]	-	✓	-	Provided solutions for allocating optimal weights along with the optimal power distribution and solved the problems using semidefinite and geometric programming.
	[218]	-	✓	-	Proposed a CJ strategy to deal with eavesdroppers anywhere in the wireless network. Also, introduced jammer placement algorithms targeted towards optimizing the total number of jammers.
	[219]	✓	-	-	Proposed a secrecy sum rate maximization based matching algorithm between primary transmitters and secondary cooperative jammers. Also, the conventional distributed algorithm (CDA) and the pragmatic distributed algorithm (PDA) are modified for maximizing the secrecy sum rate for the primary user.
	[220]	-	✓	-	Proposed a social-aware cooperative jamming strategy along with optimal power allocation scheme.
	[221]	✓	-	-	Proposed two models namely, single-channel multijammer (SCMJ) model and the multichannel single-jammer (MCSJ) model. Also, derived a closed-form expression for the optimal price strategy for Bertrand equilibrium.
Multiple	[222]	-	✓	-	Proposed a two-hop transmission protocol to ensure secure and reliable big data transmissions in wireless networks with multiple eavesdroppers.
	[223]	-	✓	-	Formulated stochastic geometry based analytical model when the location of eavesdroppers is unknown.
	[224]	-	✓	-	Proposed a friendly jammer-assisted user pair selection (FJaUPS) scheme to improve the security-reliability tradeoff.
	[225]	-	✓	-	Proposed a Gauss-Jacobi iterative algorithm to compute a Stackelberg Equilibrium
	[226]	-	✓	-	Derivation of closed-form expression for the secrecy outage probability and establishing the condition under which positive secrecy rate is achievable. Also provided a secure transmit design for maximizing the secrecy outage probability constrained secrecy rate.
	[227]	-	✓	-	Derivation of feasibility condition to achieve a positive secrecy rate at the destination to solve the secrecy rate maximization problem. Also, an iterative algorithm is developed to obtain the optimal power allocation at the jammers.
	[193]	-	✓	-	Proposed a heuristic genetic algorithm based solution followed by low complexity optimization solutions by considering the upper and lower bounds of power allocation.
	[228]	-	✓	✓	Proposed a suboptimal power allocation solution for jammer nodes for various scenarios, location of the eavesdroppers, and the destination.
	[229]	✓	-	-	Proposed an algorithm based on the monotonic optimization and the semidefinite programming (MO-SDP).

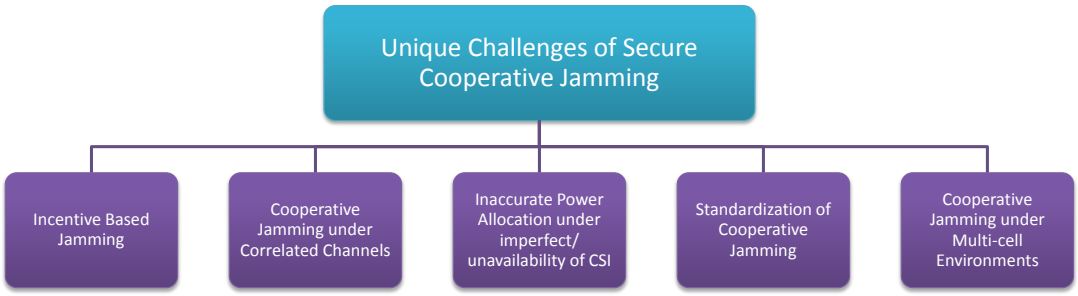


Fig. 16: Various challenges of cooperative jamming approaches.

to obtain the CSI and location of an eavesdropper if it lies in the nearby cell or if it is moving from one cell to another. To our best knowledge, very limited work has been done to investigate the secrecy performance under multi-cell environment [244]. Hence, in view of its practical importance, considerable attention needs to be paid to propose dynamic jamming protocols.

V. Hybrid Cooperation Schemes

Above mentioned sections consider cooperative relaying and jamming separately, however, there exist studies in PLS that jointly exploit the advantages of relaying and jamming, as given in Table VII. To cover these studies, we provide an overview of hybrid techniques that jointly discuss relaying and jamming strategies.

A. Joint Relay/ Jammer Selection

One important area of research in PLS is the *secure relay and jammer selection*. The secrecy outage probability may tell us about the status of the relay whether it can be trusted or not [135]. In most parts of literature, relay and jammer selection is either not made, or if made, its broadcast to other relays, possibly leading to an eavesdropper. The destination having the information of only main link and statistics of eavesdropper will select optimal relays and jammer. Each node computes a channel coefficient and compares it to a threshold. If it is above the threshold, it acts as a relay and if below, it acts as a jammer. The optimal relay and jammer can be selected by an exhaustive method. Specifically, *Greedy method* and *Vector Alignment* technique are used for optimal relay and jammer selection. The SOP decreases as the authors compare different cases, such as no jammer, random selection, greedy method, vector alignment method and finally exhaustive search. The results show that even though exhaustive search is best for SOP, it requires very thorough search.

Information theoretic security performance was investigated in [258], [259], [87], [260], [261], [262] for AF relaying and destination-assisted jamming. He *et al*. in [83] deduced that positive secrecy rate can be achieved in the presence of an untrusted relay. Particularly, the authors considered destination assisted jamming during the source to relay communication. Huang *et al*. considered friendly jamming approaches, along with relaying to perform secure communication [263]. Wang *et al*. in [258] consider the case of the best relay selection to improve the secrecy performance, in the presence of multiple eavesdroppers. The best relay selection strategy is compared with a suboptimal scheme to combat eavesdroppers. The system model is then extended to incorporate a friendly jammer in the network. It was concluded, through simulation and analytical results, that the secrecy can be increased by increasing SNR between relay and destination and between jammer and eavesdroppers.

The authors in [264] proposed a game theoretic model by formulating two Stackelberg games to solve the problem of secrecy rate maximization. It was proved that Stackelberg equilibrium exists, and was corroborated by simulation results. The Stackelberg equilibrium was found to be an efficient solution to maximize the secrecy rate. In addition to this, the authors also proposed a multi-jammer assistance strategy to save energy, while providing improved secrecy in wireless networks.

According to Ding *et al*. CJ can be used to enhanced PLS, by performing antenna selection, along with AN [265]. A pair of source nodes, relay and eavesdropper is considered. All nodes have multiple antennas. The AN is added and the performance is evaluated again by adding more AN and joint antenna selection improvement to improve the secrecy rate. As the magnitude of AN is increased, the eavesdropper channel is degraded and secrecy rate is increased. The simulations are performed for a number of scenarios and it was found that the probability to have zero secrecy rate reduces as the number of antennas increases.

The authors of [266] proposed a novel transmission scheme for energy harvesting untrusted relays, as shown in Figure 17. Particularly, if the instantaneous secrecy rate of the main link lies above a targeted secrecy rate then direct single-hop transmission (DSHT) mode is selected otherwise cooperative relaying dual-hop transmission (RDHT) mode is used. If the DSHT mode is used, then the jammer injects the jamming signal to degrade the reception of relaying nodes while causing no interference in the main channel. In case the RDHT mode is selected, then during the transmission of message from source to relay, both destination and jammer transmit jamming signals. During the second slot, if only one of the relays is active then that relay is selected to transfer the message to the destination. However, only the jammer transmits the jamming signal during this time while the destination node refrains from confusing the relays. The authors noted that there is a tradeoff between the amount of harvested energy and the secrecy performance. Specifically, they showed that the SOP

TABLE VII: Overview of recently proposed solutions for cooperative relaying and jamming.

Eavesdropper(s)	Reference(s)	Single Jamming Node	Multiple Jamming Nodes	Destination Assisted Jamming	Solution
Single	[245]	✓	-	-	Proposed a FD jamming relay network in which the relay node transmits jamming signals while receiving the data from the source.
	[246]	✓	-	✓	Proposed two transmission schemes i.e. (1) direct transmission scheme (DTS) with jamming and (2) relay transmission scheme (RTS) and compare both schemes in terms of ergodic secrecy rate.
	[247]	-	✓	-	Proposed transmit weight optimization of CR and CJ for with and without the availability of eavesdroppers' CSI.
	[248]	✓	-	-	Derivation of closed-form jamming beamformers and the corresponding optimal power allocation. Also, proposed GSVD-based secure relaying schemes for the transmission of multiple data streams.
	[249]		✓	-	Proposed a sequential parametric convex approximation (SPCA) algorithm to locate the Karush-Kuhn-Tucker (KKT) solution for maximization of ergodic secrecy rate.
	[250]	-	✓	-	Proposed power allocation technique for transmitting jamming signals, secondary messages, and relaying messages such that the secrecy capacity of the primary system is maximized subject to the minimum secondary user transmission rate requirements.
	[251]	-	✓	-	Proposed heuristic algorithm to solve joint problems of subcarrier assignment, subcarrier pairing and power allocations under scenarios of CJ to maximize the secrecy sum rate subject to limited power budget at the relay.
	[252]	-	✓	-	Proposed a worst-case robust design by considering imperfect CSI of eavesdropper to obtain distributed jamming weights, which is solved through semi-definite program (SDP).
	[253]	-	✓	-	Proposed an optimal relay selection scheme for (1) full CSI, (2) partial CSI and (3) statistical CSI cases. Also, exact and approximate secrecy outage probability expressions in closed-form are derived.
	[254]	-	✓	✓	Proposed a joint relay and jammer selection scheme and derive a closed-form suboptimal solution to maximize the secrecy rate.
	[255]	✓	-	-	Proposed an adaptive cooperative relaying and jamming secure transmission scheme to protect the confidential messages where the legitimate receiver adopts the energy detection method to detect the jamming-aided eavesdropper's action and a cooperative node aid the secure transmission through cooperative relaying under jamming attack under eavesdropping attack.
	[256]	-	✓	-	Proposed a bi-level optimization algorithm for deriving the optimal jamming and beamforming vector.
	[257]	-	✓	✓	Proposed a scheme for jointly optimizing the bandwidth and time in DF relaying while satisfying the secrecy requirements through jamming.
Multiple	[135]	-	✓	-	Derivation of a closed-form expression for the secrecy outage probability and developed two relays and jammer selection methods for minimization of secrecy outage probability.
	[16]	-	✓	✓	Derivation of a closed-form solution for the optimal power allocation and proposed a simple relay selection criterion under two scenarios of non-colluding and colluding eavesdroppers.

increases for RDHT when the relays are closer to source, however, the amount of harvested energy is significantly high. On the contrary, if the relays are farther from the source and closer to the destination, then the SOP decreases as the first hop becomes a bottleneck for RDHT and limited energy harvesting takes place at the relays.

Ibrahim *et al*. in [267] proposed three categories of relay and jammer selection for two-way cooperative communication scenario. The authors also introduced schemes to overcome the negative effects of interference. The authors concluded that the cooperation of eavesdroppers further degrades the secrecy outage performance. It was also shown that two-way relaying outperforms one-way relaying schemes.

The PLS highly depends on the CSI; the perfect knowledge of CSI is required to make sure that the eavesdropper gets the least of the legitimate information. In most of the work done in PLS, the CSI is assumed to be known at the transmitter. The CSI can only be estimated at the receiver, and the knowledge of CSI is required at the transmitter so the used AN can be targeted at the eavesdropper and nullified at the legitimate receiver. Feeding back the CSI, from the receiver to the transmitter, is common practice. This feedback takes time and since the channel is variable it may affect the performance of secrecy algorithms [268]. The authors consider DF protocol for intermediate relays, while Rayleigh fading is considered. In step 1, the transmitter forwards the signal to relays at while in step 2, the relays forward the signals. The SOP and secrecy rate depend upon the delay, where the CSI is fedback. It is demonstrated that with an increase in the feedback delay, the SOP also increases.

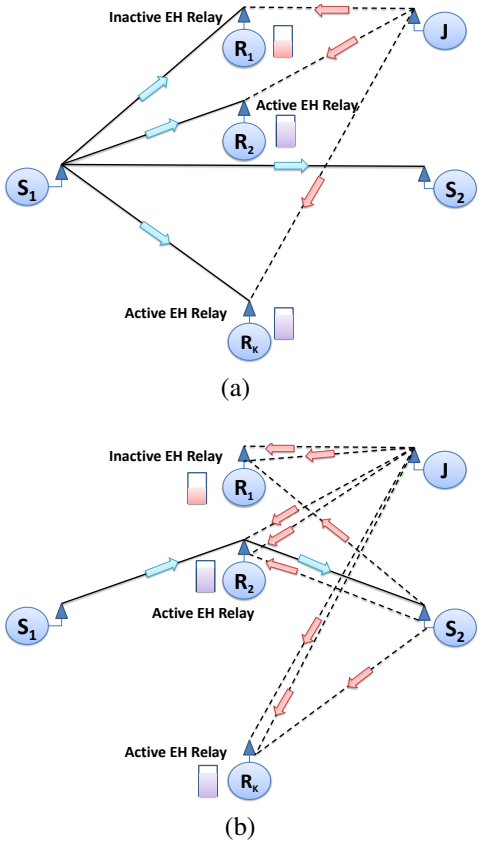


Fig. 17: Secure communication with untrusted relaying (a) DSHT (b) RDHT [266].

B. Joint Power Allocation

For wirelessly powered networks, the secrecy performance was evaluated by Xing *et al*. in [269]. Multi-antenna AF relaying was considered for hybrid receiver architecture. The received power is split into two streams for energy harvesting and information decoding. The communication is conducted into two phases where the first phase is used for energy harvesting and the second phase is used for jamming. The power reserved during the first phase is used for jamming in the second phase. Note that the authors assume that the density of eavesdroppers is known at the relay and CSI of eavesdroppers is not available. The results unveil that maximum ergodic secrecy rate is achieved for shorter relay-destination distances.

For the case of multiple helpers, the secrecy performance of harvest and jam (HJ) protocol was evaluated in [270]. Similar to above-mentioned approach, the radio signal is transferred to AF relay during first phase, which is used to harvest energy and decode information. A group of helpers, equipped with multiple antennas, use the harvested power to generate AN and degrade the signal of an eavesdropper. The secrecy rate is maximized by optimizing covariance matrix and its performance is compared with heuristic schemes. It has been shown that the performance of the proposed scheme is significantly improved when helpers are equipped with a larger number of antennas.

Similar to the work of [270], Xing *et al*. in [271] provided an optimal solution to reduce the complexity of receivers. The authors also presented semi closed-form solution to perform null space jamming. For perfect CSI availability cases, the authors show that the derived semi-definite relaxation (SDR) closely follow the simulation results. In contrast, for the case of imperfect CSI, a suboptimal rank algorithm was provided.

Xiao *et al*. in [272] studied two eavesdropping conditions of untrusted relay, i.e. active eavesdropping and non-active eavesdropping. Subsequently, the authors used Lagrange duality methods to decompose the optimization problem in two sub-problems. In particular, the authors jointly optimized power splitting ratio while minimizing the outage probability. It has been shown by the authors that the system performance is improved for non-active mode, as compared to the proactive mode.

C. Joint Relay/ Jammer Beamforming

A two-way relay network offering a practical case and a study of the PLS in such networks is quite interesting. *Hybrid cooperative beamforming and jamming* can be combined with two-way relays. The intermediate terminals act as a relay and also do the beamforming [273]. The secrecy rate is increased by optimizing the weights of beamforming and jamming vectors. Here the authors assume a transmitter-receiver pair, N relay nodes and J eavesdroppers. Each node has single antenna and the relay operates in FD mode. Communication channel between all possible pairs is assumed to be flat. One communication round is split into broadcasting phase and beamforming phase. In first stage, the source broadcast a message signal (two-way). The relay broadcast a weighted jamming signal to confuse the interceptor. The receiver has full CSI, so it separates the original message signal from the jamming signal.

CB and CJ can be combined to perform efficiently, in order to select the optimal nodes to serve as relays and jammers. In this regard, an SDR solution for secrecy rate maximization problem is considered feasible. The secrecy scaling laws for a large number of nodes were analyzed in [111]. The authors in [274], designed optimal precoding matrices for a MIMO relay channel. Similarly, source GSVD and relay SVD precoding was introduced in [98] to improve the secrecy performance of cooperative networks.

With two-way relay nodes, a rather practical scenario is considered and with a hybrid technique, the multi-antenna requirement is reduced and secrecy rate are improved. Secrecy rate can be improved when beamforming and jamming is used jointly [275]. The CB improves transmitter to receiver channel secrecy capacity, whereas CJ degrades wiretap link secrecy rate. Multiple nodes perform CB to increase the secrecy rate. Because of two-phase transmission, the eavesdropper get two chances to degrade the quality of the main link. This is achieved with some intermediate nodes doing beamforming while other doing jamming. *Null-space beamforming* is used to optimize the power constraints of all terminals.

For energy harvesting networks, the destination-assisted jamming for untrusted intermediate relay was studied in [276]. Specifically, the destination node uses the harvested energy

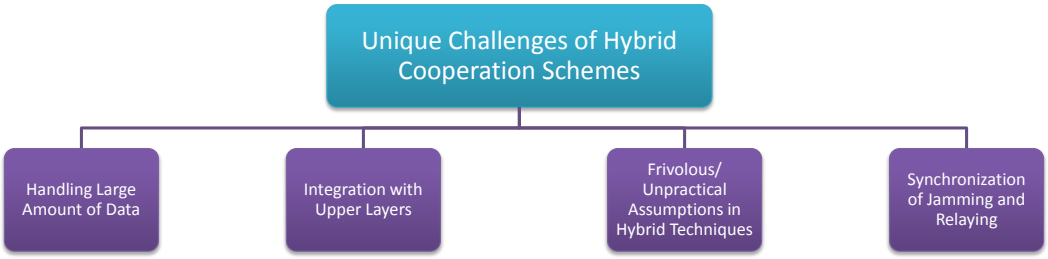


Fig. 18: Research challenges of hybrid cooperation schemes.

during first transmission phase to jam the transmission of the untrusted relay. The results demonstrated in the paper unveil that power splitting policy achieves better optimal secrecy performance as compared to time switching policy.

D. Unique Challenges of Hybrid Cooperative Approaches

Let us now discuss some of the challenges pertaining to joint utilization of relays and jammers, as shown in Figure 18.

1) Handling Large Amount of Data: The integration of hybrid cooperative strategies comes with an excessive cost of repeated data processing. With a demand of higher data rates, the cooperation of nodes must be flexible enough to handle a large amount of data. This much processing of data would undoubtedly increase the energy consumption, creating a bottleneck if the devices start dying more frequently. Resultantly, more efforts should be put into designing protocols with enhanced capabilities and efficiency.

2) Integration with Upper Layers: One of the interesting directions for joint relaying and jamming is to exploit higher layers for efficient routing of messages. So far, the research efforts in relaying and jamming are mostly limited to physical layer techniques. However, there is a need to emphasize on the routing schemes to minimize intermittent connectivity issues during relaying and jamming. It is because the reachable neighbors of a node can vary rapidly for mobile networks. Moreover, the issue of intermittent connectivity can also result in rerouting of the messages through intermediate relays. The secrecy performance of these hybrid schemes under retransmissions and under the influence of upper layers anomalies is still undiscovered. The same is essential from design perspective of practical systems using these hybrid schemes.

3) Frivolous/ Unpractical Assumptions in Hybrid Techniques: The existing hybrid techniques in PLS literature usually consider a very basic premise with specific number of nodes. It is mostly assumed that the distance between the jammers is relatively smaller than the distance between source/eavesdropper/destination [254]. Some works consider perfect knowledge of wireless channels [277], [135], [278]. These assumptions, though necessary for tractable analysis, oversimplify the system model to an extent that no longer remains practical. Moreover, the optimization strategies proposed under these assumptions may not produce the same results or work effectively if implemented on hardware.

4) Synchronization of Jamming and Relaying: One of the most neglected factors in hybrid techniques is the issue of time synchronization of the jammer and relays. It is worth mentioning that these hybrid techniques generally consider block fading models. According to the block fading model, the channel remains unchanged for a particular coherence time, while it randomly changes from one block to another. This consideration is fairly genuine, yet the devices far away from each other may not have same length the fading block. Resultantly, time synchronization based on block fading model is not much practical. Moreover, hardware requirements for precise synchronization and the impact of imperfect timing synchronization is majorly unknown.

VI. Future Applications of Cooperative PLS

One of our paper's goal is to understand how cooperative relaying and jamming can be applied to different forthcoming wireless technologies, to improve the PLS. More specifically, we discuss the recent studies and provide some key challenges and issues in the system design.

A. Wireless Information and Power Transfer Cooperative Networks

Recently, simultaneous wireless information and power transfer (SWIPT) have generated significant research interest from academia and industry [279], [280], [281], [282]. It can increase the lifetime of energy limited devices in the network. In fact, SWIPT improves the functionality of conventional wireless networks by concurrently transmitting power and information at the receiver. The source transfers power and information signal in a unicast (dedicated) or multicast scenario, as shown in Figure 19. In point to point communication, this approach is not much feasible if the same receiver is used for information decoding (ID) and energy harvesting (EH). It is because the power receiver needs to be placed near the source due to latter's lower sensing ability. Therefore, instead of point to point communication, intermediate relays can be used to improve the performance of the network, in terms of lifetime and reliability. The relay can be charged using one of these methods: 1) using dedicated power transfer source 2) using power splitting (PS) [283], [284], time switching (TS) [285] or antenna selection (AS) [286] receiver architecture. If the relay uses a dedicated power source then the secrecy rate at the relay is similar to conventional relaying networks.

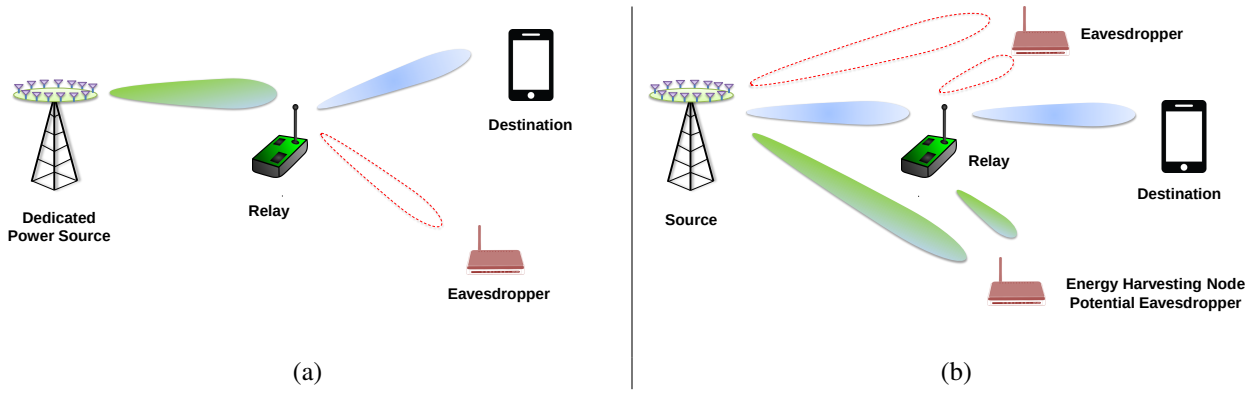


Fig. 19: Cooperative security scenarios (a) Dedicated power transmission (2) Simultaneous wireless information and power transfer.

In contrast, when the relay uses the received RF signal to simultaneously harvest energy and decode information, then the secrecy rate depends on any one or all of the PS/ AS/ TS factors.

A fundamental three-node network model was considered in [287] in which the information eavesdropper was also a legitimate network node but with a limited role of only energy harvesting from the received RF signal. However, the eavesdropper additionally engaged in the un-authorized activity of intercepting the secret communication between the legitimate nodes. An optimization strategy was proposed for transmit beamforming to improve the secrecy of the legitimate users. The previous model was extended to a four-node scenario in [288], [110] and the secrecy performance was analyzed. In particular, as shown in Figure 20, the authors of [110] noted that a large power splitting factor increases the intercept probability. Furthermore, the authors also concluded that for smaller values of the time-allocation factor, the system's secrecy performance can be ensured by allocating less power at the relaying node for energy harvesting and more power for decoding the received information. The authors in [270], [289], [271] using AF relaying and jamming techniques, improved the secrecy performance under PS architecture of ID and EH. In a similar way, the authors provided a robust security scheme by using AN in [290]. The case for multiple power receiver i.e. multiple energy harvesting eavesdroppers, was considered in [291], wherein, two problems were addressed 1) maximization of secrecy rate for information receiver and 2) maximization of energy transferred subject to secrecy rate constraint. Some recent studies also show that security and energy efficiency, in power transfer networks, can be improved by deploying friendly jammers. The authors in [292] improved the PLS by introducing an extra jamming node in the network. More specifically, CJ optimization was performed for the worst case secrecy rate. The authors in [266] provide a cooperative relaying and jamming scheme for untrusted dual-hop energy harvesting AF relays. Cooperative relaying to enhance the secrecy of devices was improved in SWIPT, in [293]. The authors consider multiple antennas to minimize information leakage and maximize harvested energy. Massive MIMO systems with SWIPT were studied in [294] and it was illustrated that large antenna gains can be used to

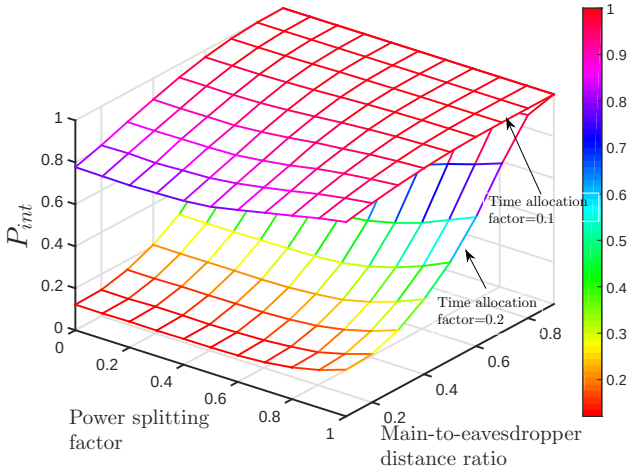


Fig. 20: Intercept probability against power splitting factor [110].

improve the efficiency of transferred power. Moreover, high resolution beamforming was used to significantly decrease the pilferage of information. Similarly, energy efficient mechanism in SWIPT enabled massive MIMO was studied in [295] and an efficient power allocation scheme was proposed to provide link security.

B. Massive MIMO

Massive MIMO is a type of multi-user MIMO scheme in which the BS is equipped with hundreds of antennas and can serve tens of users in the same time-frequency block. In [296] the authors proved that by using a very large number of antennas at the BS even simple linear processing performs near optimal; e.g., by using MRC in the uplink or maximum-ratio transmission (MRT) in the downlink, the effects of fast fading, inter-cell interference, and uncorrelated noise almost vanish in the limit of a large number of BS antennas. The key question here is whether significant multiplexing gain can be obtained with low complexity and low-cost signal processing techniques.

In contrast to traditional MIMO, the massive MIMO systems have more stringent security challenges. Firstly, the process of CSI estimation in massive MIMO is complex due

to a large number of antennas. Secondly, the antennas may experience correlated fading due to potentially small inter-element spacing and then the conventional independent fading models cannot be used. This also introduces complications in the derivation of analytical expressions. Lastly, the pilot contamination can adversely affect channel estimation and thereby degrade the secrecy performance of the system. To partly address this issue, the authors in [297] derived an asymptotic expression of secrecy capacity by jointly using AN precoding and ZF in massive MIMO systems. Zhu *et al*. in [298] analyzed the secrecy capacity for multi-cell massive MIMO systems. For cooperative massive MIMO systems, the analysis of secrecy outage was performed in [96], [42]. Wang *et al*. in [299] provided the optimal power allocation factor to reduce the secrecy outage probability. The authors in the same work also proposed directional jamming towards the eavesdropper. The authors concluded that directional jamming outperforms conventional omnidirectional jamming in massive MIMO systems. A jamming signal detection strategy for massive MIMO network was provided in [300]. It was concluded that a receiver node can more efficiently reject the jamming signal if its desired signal has a significantly larger power level compared with that of the jamming signal.

In a similar study [301], the authors considered a single cell with a single-antenna jammer that could adjust its transmit power. The authors then proposed a receiver filter to reduce the impact of jamming in the considered scenario. However, the generalized case for multi-cell environment in the presence of an N-antenna jammer was considered in [302]. For such scenarios, the BS must estimate N channels and subsequently cancel the interference from these channels. In this case the exploitation of frequency/time offsets or subspace methods may prove more suitable for jamming signal rejection.

C. Internet of Things (IoT)

There is estimated to be up to 20 billion IoT device by 2020 whereby these devices are predicted to generate a revenue of US$ 9.8 trillion [303]. Despite its applications in health and autonomous drones and logistics, there are still weaknesses in their core design with respect to implementation of IoT. The first weaknesses arise due to the configuration of IoT devices [304], [305], [306]. The process of reconfiguration is a delicate one as it needs to be performed on secure channel or the eavesdropper may acquire sensitive information, such as keys and device association. The second challenge comes from the lack of well-defined topology of IoT networks, and due to the fact that IoT network may consist of both static and mobile nodes. Consequently, it is not possible to arrange devices in a specific order to fully exploit cooperation of nodes at physical layer.

The work on link security of IoT networks is still in early stages and only limited number of studies exist in the literature [307]. Pecorella *et al*. in [308] proposed a physical layer based method to improve the link security/ reliability of data, without extra hardware or increased complexity. However, the proposed scheme is found to be more suitable for near-field transmission scenario. Still the work on cooperative schemes in IoT, to ensure secrecy of messages, is non-existent and more efforts are required to be focused towards the physical layer aspect of the IoT.

D. Spectrum Extension (mm-Wave/ FSO)

In recent years, research efforts are being made to exploit the spectrum bands, not used in the earlier generation of networks. A very promising solution for future 5G cellular network is the mmWave communication [309]. The mmWave contains a wide range of carrier frequencies, operating over a frequency band of 3-300 GHz. It provides short range, high bandwidth (multi-gigabits-per second) connectivity for cellular devices. The mmWave band has several desirable features, including large bandwidth, compatibility with directional transmissions, reasonable isolation, and dense deployability. The mmWave channels suffer from significant attenuation due to the inability of short mmWave band wavelengths to diffract around obstacles. Interruption in line of sight (LoS) communication, due to a moving obstacle, can lead to link outage in this case [258]. Further, the limited penetration capability could restrict the mmWave connectivity to a confined space. For example outdoor mmWave signals may be confined to outdoor structures, such as car parkings or streets, and limited signals may penetrate inside buildings [258], [310]. Recently, Gong *et al*. considered two-way relaying for mmWave band in [311], [312]. Secrecy performance of ad-hoc networks, using mmWave band, was evaluated by Zhu *et al*. in [313], [310] while [314] designed precoders for MISO OFDM systems using mmWave band.

Similar to mmWave, Free-Space Optical (FSO) communication [315] is also expected to provide many enhancements in bandwidth utilization. However, like mmWave, FSO also faces challenges due to heavy rain and fog. Also the performance of FSO completely degrades in non-LOS condition [316]. In the context of PLS, [141] discussed a link security in a hybrid RF/FSO multiuser relay network. More specifically, security-reliability tradeoff was discussed by the authors, followed by providing opportunistic scheduling schemes. It was found that the information leakage takes place if the eavesdropper is located near the receiver or transmitter, without affecting the reliability of information transfer. Link security analysis for FSO system over Malaga Turbulence channels was provided in [317]. Similarly, the secrecy performance of RF/FSO system was also evaluated in [12], where the authors consider Nakagami-m fading for RF link and Gamma-Gamma fading for FSO link.

E. Device-to-device (D2D) Communication

A rapid increase in the density of devices has pushed up the demand of data rates in wireless communication. In this regard, D2D communication, which allows direct communication between two-user equipments (UEs), has emerged as a prominent technology for upcoming cellular networks [318], [319], [320]. Specifically, proximity gains can be used to improve energy and spectrum efficiency. This brings up the challenges of high interference to conventional cellular user equipment (CUE) causing a performance degradation.

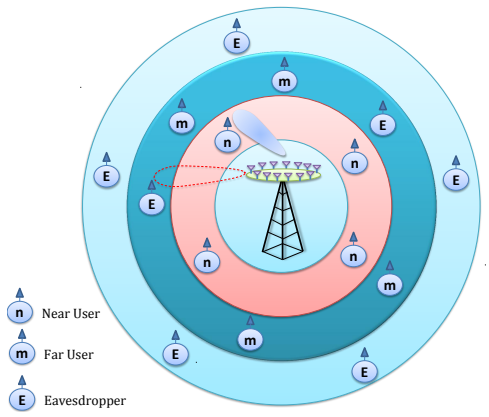


Fig. 21: Protected zones for cooperative NOMA in the presence of multiple eavesdroppers.

This interference can be used to significantly enhance the link security of cellular networks [321], [322], [323]. Also, when generated by a friendly D2D jammer, it can be used to confuse the eavesdropper, allowing the D2D user to transmit frequently.

The authors in [324] jointly optimized the access control and power of RF link, where the links were subjected eavesdropping attacks. The authors then provided an extension to their work, by applying the same optimization strategy for large-scale D2D networks in [325]. For the case of multiple eavesdroppers and multiple antennas, Chu *et al*. in [326] considered a downlink D2D communication scenario to provide a robust beamforming technique. The authors in [324], optimized access control and transmit power subject to secrecy constraints for CUEs. This case was extended for a large scale D2D network in [325]. The authors introduced a scheduling strategy for D2D links to improve their secrecy performance. A generalized $M \times N$ relay-assisted D2D scenario was considered by the authors in [327], where N represents the number of cluster of devices and M denotes the number of devices in each cluster. It was unveiled that the SOP increases an increase in the number of hops. In contrast, it decreases as the number of devices in each cluster increase. A robust MISO beamforming technique was proposed in [326] to maximize the secrecy rate and minimize the transmit power, under the constraint of transmission rates.

F. Non-orthogonal multiple access (NOMA)

Non-orthogonal multiple access (NOMA) is deemed to be a revolutionary advancement for future 5G networks. NOMA allows users with better wireless channel conditions to apply successive interference cancellation (SIC) techniques to remove the messages for other users, and subsequently decode their messages [328]. From the perspective of cooperative NOMA, performance of near and far users have been extensively investigated in [329], [330], [331], [332], [333], [334], [335], [336]. From the perspective of the PLS, however, limited work exists in cooperative NOMA. Cooperative NOMA scheme was considered in [337]. The authors showed that the diversity order of the system is determined by the secrecy performance of the user with a poor channel. The authors also proposed to enlarge protected zones to enhance the secrecy. In [338] authors proposed protected zones around BS by using channel ordering, as shown in Figure 21. The authors concluded that the secrecy performance of NOMA can be improved by generating AN at BS, and using pre-specified protected zones. The authors also derived exact and asymptotic closed-form expressions of the SOP. Despite these efforts, the work on secure communication in cooperative NOMA architecture is still in early stages and the secrecy enhancement of users with poor channel conditions is a critical problem. More recently, the authors in [339] proposed to enhance the secrecy performance of two-way FD relaying in a NOMA-based system. They derived closed-form expressions for the ergodic secrecy rate with and without eavesdropper collusion. It was also shown that the link reliability increases with an increase in the number of antennas at the FD relay. In [340], the authors showed that the asymptotic secrecy outage probability of DF and AF NOMA-based relays becomes constant at high SNR values. Interestingly, the authors also noted that the secrecy performance of a cooperative NOMA system is independent of the channel between the far user and the relay.

G. Cognitive Radio Networks

Spectrum scarcity is one of the most researched issues in wireless communications. In this context, cognitive radio (CR) network has been considered as a potential contender to address this issue. CR network works by allocating same spectrum to a secondary network if the QoS is not degraded or the spectrum is idle [341], [342], [343]. Since various devices are allowed to access the spectrum, therefore, CR networks are inherently vulnerable to eavesdropping attacks [344], [345], [346]. Link security of both primary and secondary users has been extensively discussed in recent years [347], [348]. A four node scenario was considered in [349], where transmit beamforming was used for multi-antenna CR transmitter. Three suboptimal and lightweight solutions were provided, due to the non-convexity of the utility function. Maji *et al*. evaluate secrecy of CR network and provide relay selection schemes under the influence of interference from neighboring nodes [350]. The problem of the information's interception was considered in [351], for multiuser cooperative CR network. Interestingly, Pareto resource allocation policies were designed for 1) maximization of energy harvesting efficiency, 2) minimization of transmit power and 3) minimization of the ratio between power leakage and total transmit power. Cooperative relaying was studied for CR in [352]. In particular, the relays were given two roles i.e., information relaying and CJ. Cooperative relaying for energy harvesting cognitive networks was studied in [353] for PS architecture. For AN aided EH cognitive networks, a precoding scheme was provided by authors in [351], to maximize the secrecy rate while minimizing interference. Similarly, opportunistic cognitive relaying was studied in [354] where one relay transmits the information to destinations, while the other relay act as a jammer for the eavesdropper. The authors provided four relay selection policies, based on different combinations

of best and random relay selections. It was then shown that secrecy outage saturation results when jamming relays are not present. The case without jamming was considered in [355]. The authors provided in-depth analysis on security-reliability tradeoff for different relay selection schemes. As demonstrated, the tradeoff between reliability and security can be minimized with an increase of relays and by adopting a proper relay selection method.

In the domain of cognitive networks, machine type communication (MTC) or machine-to-machine (M2M) communication has gathered considerable research interest. It refers to the exchange of information among devices without involvement or intervention of humans. It has numerous unique attributes that include distinct service environment, infrequent transmission of data and large-scale distribution. Recently some studies have investigated this domain, from the perspective of PLS [356], [357]. The future directions include minimization of power consumption when providing hop-to-hop link security and estimation of local and global CSI for secure route selection.

VII. Conclusion

This survey provides a detailed, transparent and precise information regarding the latest developments on the use of cooperative techniques for improving PLS. Moreover, this survey offers classification for different cooperative techniques, along with the discussion of their merits and demerits. The article also presents and elaborates different hybrid approaches and their associated challenges. Based on above stated arguments, the following key conclusion can be extracted:

- More research efforts need to be focused towards exploiting relay positioning and formulation of efficient trust metrics.
- Cross layered schemes can be used to gain more benefits from secure cooperative schemes.
- In order to efficiently utilize existing cooperative schemes, social models and incentive-based techniques need to be designed.
- Hardware implementation of hybrid cooperative schemes is still a challenge due to weak time synchronization between relays and jammers.
- Multi-cellular design needs to be further investigated for practical realization of secure cooperative PLS architecture.

Conclusively, this article provides the readers with an opportunity to appreciate the significant and rapid advances in cooperative PLS literature, which is a growing area of wireless communication. This survey will undoubtedly trigger and motivate the interested readers to concentrate their research efforts towards the design of secure cooperative PLS schemes for 5G networks.

Acknowledgment

This work is supported by the EU-funded project ATOM-690750, approved under call H2020-MSCA-RISE-2015.

References

[1] O. G. Aliu, A. Imran, M. A. Imran, and B. Evans, "A survey of self organisation in future cellular networks," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 1, pp. 336–361, 2013.

[2] F. I. Kandah, O. Nichols, and L. Yang, "Efficient key management for Big Data gathering in dynamic sensor networks," in *International Conference on Computing, Networking and Communications (ICNC)*. IEEE, 2017, pp. 667–671.

[3] A. D. Wyner, "The wire-tap channel," *Bell Labs Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[4] L. H. Ozarow and A. D. Wyner, "Wire-Tap Channel II," *Bell Labs Technical Journal*, vol. 63, no. 10, pp. 2135–2157, 1984.

[5] L. Kong, G. Kaddoum, and D. B. da Costa, "Cascaded α-μ fading channels: Reliability and security analysis," *IEEE Access*, 2018.

[6] G. De Meulenaer, F. Gosset, F.-X. Standaert, and O. Pereira, "On the energy cost of communication and cryptography in wireless sensor networks," in *International Conference on Wireless and Mobile Computing, Networking and Communications*. IEEE, 2008, pp. 580–585.

[7] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wire-tap channel," *IEEE transactions on information theory*, vol. 24, no. 4, pp. 451–456, 1978.

[8] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE transactions on information theory*, vol. 24, no. 3, pp. 339–348, 1978.

[9] M. Bloch, J. Barros, M. R. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, 2008.

[10] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4687–4698, 2008.

[11] N. Bhargav, S. L. Cotton, and D. E. Simmons, "Secrecy capacity analysis over $\kappa--\mu$ fading channels: Theory and applications," *IEEE Transactions on Communications*, vol. 64, no. 7, pp. 3011–3024, 2016.

[12] H. Lei, Z. Dai, I. S. Ansari, K.-H. Park, G. Pan, and M.-S. Alouini, "On Secrecy Performance of Mixed RF-FSO Systems," *IEEE Photonics Journal*, vol. 9, no. 4, pp. 1–14, 2017.

[13] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 21–27, 2015.

[14] L. Kong, J. He, G. Kaddoum, S. Vuppala, and L. Wang, "Secrecy analysis of a MIMO full-duplex active eavesdropper with channel estimation errors," in *Vehicular Technology Conference (VTC-Fall), 2016 IEEE 84th*. IEEE, 2016, pp. 1–5.

[15] Y. J. Tolossa, S. Vuppala, G. Kaddoum, and G. Abreu, "On the Uplink Secrecy Capacity Analysis in D2D-Enabled Cellular Network," *IEEE Systems Journal*, 2017.

[16] A. Kuhestani, A. Mohammadi, and M. Mohammadi, "Joint relay selection and power allocation in large-scale mimo systems with untrusted relays and passive eavesdroppers," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 2, pp. 341–355, 2018.

[17] M. Mirmohseni and P. P. Papadimitratos, "Secrecy Capacity Scaling in Large Cooperative Wireless Networks," *IEEE Transactions on Information Theory*, vol. 63, no. 3, pp. 1923–1939, 2017.

[18] G. Chen, J. P. Coon, and M. Di Renzo, "Secrecy outage analysis for downlink transmissions in the presence of randomly located eavesdroppers," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 5, pp. 1195–1206, 2017.

[19] Y. Feng, Z. Yang, W.-P. Zhu, Q. Li, and B. Lv, "Robust cooperative secure beamforming for simultaneous wireless information and power transfer in amplify-and-forward relay networks," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 3, pp. 2354–2366, 2017.

[20] P. C. Pinto, J. Barros, and M. Z. Win, "Secure communication in stochastic wireless networksPart I: Connectivity," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, pp. 125–138, 2012.

[21] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, Technologies, and Challenges," *IEEE Communications Surveys & Tutorials*, 2016.

[22] G. Verma, P. Yu, and B. M. Sadler, "Physical layer authentication via fingerprint embedding using software-defined radios," *IEEE Access*, vol. 3, pp. 81–88, 2015.

[23] L. Y. Paul, G. Verma, and B. M. Sadler, "Wireless physical layer authentication via fingerprint embedding," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 48–53, 2015.

[24] L. Shi, M. Li, S. Yu, and J. Yuan, "BANA: body area network authentication exploiting channel characteristics," *IEEE Journal on selected Areas in Communications*, vol. 31, no. 9, pp. 1803–1816, 2013.

[25] W. Hou, X. Wang, J.-Y. Chouinard, and A. Refaey, "Physical layer authentication for mobile systems with time-varying carrier frequency offsets," *IEEE Transactions on Communications*, vol. 62, no. 5, pp. 1658–1667, 2014.

[26] K. M. Borle, B. Chen, and W. K. Du, "Physical layer spectrum usage authentication in cognitive radio: analysis and implementation," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 10, pp. 2225–2235, 2015.

[27] A. Zhang, L. Wang, X. Ye, and X. Lin, "Light-weight and robust security-aware d2d-assist data transmission protocol for mobile-health systems," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 3, pp. 662–675, 2017.

[28] L. Wang, H. Wu, and G. L. Stüber, "Cooperative Jamming-Aided Secrecy Enhancement in P2P Communications With Social Interaction Constraints," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 2, pp. 1144–1158, 2017.

[29] W. Wang, K. C. Teh, and K. H. Li, "Enhanced Physical Layer Security in D2D Spectrum Sharing Networks," *IEEE Wireless Communications Letters*, vol. 6, no. 1, pp. 106–109, 2017.

[30] Z. Shu, Y. Qian, and S. Ci, "On physical layer security for cognitive radio networks," *IEEE Network*, vol. 27, no. 3, pp. 28–33, 2013.

[31] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5g wireless communication networks using physical layer security," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 20–27, 2015.

[32] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. K. Wong, and X. Gao, "A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead," *IEEE Journal on Selected Areas in Communications*, pp. 1–1, 2018.

[33] B. He, X. Zhou, and T. D. Abhayapala, "Wireless physical layer security with imperfect channel state information: A survey," *arXiv preprint arXiv:1307.4146*, 2013.

[34] W. Trappe, "The challenges facing physical layer security," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 16–20, 2015.

[35] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014.

[36] A. Yener and S. Ulukus, "Wireless physical-layer security: Lessons learned from information theory," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1814–1825, 2015.

[37] M. Atallah, G. Kaddoum, and L. Kong, "A survey on cooperative jamming applied to physical layer security," in *Ubiquitous Wireless Broadband (ICUWB), 2015 IEEE International Conference on*. IEEE, 2015, pp. 1–5.

[38] T. M. Cover and J. A. Thomas, *Elements of information theory*. John Wiley & Sons, 2012.

[39] M. Bloch and A. Thangaraj, "Confidential messages to a cooperative relay," in *Information Theory Workshop*. IEEE, 2008, pp. 154–158.

[40] Y. Zou, J. Zhu, X. Wang, and V. C. Leung, "Improving physical-layer security in wireless communications using diversity techniques," *IEEE Network*, vol. 29, no. 1, pp. 42–48, 2015.

[41] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 10, pp. 2099–2111, 2013.

[42] X. Chen, L. Lei, H. Zhang, and C. Yuen, "On the secrecy outage capacity of physical layer security in large-scale MIMO relaying systems with imperfect CSI," in *International Conference on Communications (ICC)*. IEEE, 2014, pp. 2052–2057.

[43] M. Z. I. Sarkar, T. Ratnarajah, and M. Sellathurai, "Secrecy capacity of nakagami-m fading wireless channels in the presence of multiple eavesdroppers," in *Conference Record of the Forty-Third Asilomar Conference on Signals, Systems and Computers*. IEEE, 2009, pp. 829–833.

[44] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in MIMO wire-tap channels," *IEEE Transactions on Communications*, vol. 61, no. 1, pp. 144–154, 2013.

[45] T. C.-Y. Ng and W. Yu, "Joint optimization of relay strategies and resource allocations in cooperative cellular networks," *IEEE Journal on Selected areas in Communications*, vol. 25, no. 2, 2007.

[46] M. Yu, J. Li, and H. Sadjadpour, "Amplify-forward and decode-forward: The impact of location and capacity contour," in *Military Communications Conference, 2005. MILCOM 2005. IEEE*. IEEE, 2005, pp. 1609–1615.

[47] N. Kumar, P. K. Singya, and V. Bhatia, "Performance analysis of orthogonal frequency division multiplexing-based cooperative amplify-and-forward networks with non-linear power amplifier over independently but not necessarily identically distributed Nakagami-m fading channels," *IET Communications*, vol. 11, no. 7, pp. 1008–1020, 2017.

[48] S. Sohaib and M. Uppal, "Full Duplex Compress-and-Forward Relaying Under Residual Self-Interference," *IEEE Transactions on Vehicular Technology*, 2017.

[49] T. Yang, "Distributed MIMO broadcasting: Reverse compute-and-forward and signal-space alignment," *IEEE Transactions on Wireless Communications*, vol. 16, no. 1, pp. 581–593, 2017.

[50] H. U. Sokun and H. Yanikomeroglu, "On the Spectral Efficiency of Selective Decode-and-Forward Relaying," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 5, pp. 4500–4506, 2017.

[51] J. Jin, X.-C. Gao, X. Li, S. Li, and Z. Wang, "Achievable degrees of freedom for the two-cell two-hop mimo interference channel with half-duplex relays," *IEEE Access*, vol. 5, pp. 1376–1381, 2017.

[52] R. R. Thomas, M. Cardone, R. Knopp, D. Tuninetti, and B. T. Maharaj, "A practical feasibility study of a novel strategy for the gaussian half-duplex relay channel," *IEEE Transactions on Wireless Communications*, vol. 16, no. 1, pp. 101–116, 2017.

[53] Z. Chen, P. Fan, and D. O. Wu, "Joint power allocation and strategy selection for half-duplex relay system," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 3, pp. 2144–2157, 2017.

[54] W. Shin, N. Lee, H. Yang, and J. Lee, "Relay-aided successive aligned interference cancellation for wireless x networks with full-duplex relays," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 1, pp. 421–432, 2017.

[55] D. Wang, R. Zhang, X. Cheng, L. Yang, and C. Chen, "Relay Selection in Full-Duplex Energy-Harvesting Two-Way Relay Networks," *IEEE Transactions on Green Communications and Networking*, vol. 1, no. 2, pp. 182–191, 2017.

[56] C. Yin, T. X. Doan, N.-P. Nguyen, T. Mai, and L. D. Nguyen, "Outage probability of full-duplex cognitive relay networks with partial relay selection," in *IEEE International Conference on Recent Advances in Signal Processing, Telecommunications & Computing (SigTelCom)*, 2017, pp. 115–118.

[57] N. Zlatanov, V. Jamali, and R. Schober, "Achievable rates for the fading half-duplex single relay selection network using buffer-aided relaying," *IEEE Transactions on Wireless Communications*, vol. 14, no. 8, pp. 4494–4507, 2015.

[58] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE transactions on signal processing*, vol. 58, no. 3, pp. 1875–1888, 2010.

[59] N. Zhou, X. Chen, C. Li, and Z. Xue, "Secrecy rate of two-hop AF relaying networks with an untrusted relay," *Wireless personal communications*, vol. 75, no. 1, pp. 119–129, 2014.

[60] L. Fan, X. Lei, T. Q. Duong, M. Elkashlan, and G. K. Karagiannidis, "Secure multiuser communications in multiple amplify-and-forward relay networks," *IEEE Transactions on Communications*, vol. 62, no. 9, pp. 3299–3310, 2014.

[61] J. Yao, S. Feng, X. Zhou, and Y. Liu, "Secure routing in multihop wireless ad-hoc networks with decode-and-forward relaying," *IEEE Transactions on Communications*, vol. 64, no. 2, pp. 753–764, 2016.

[62] J. Chen, R. Zhang, L. Song, Z. Han, and B. Jiao, "Joint relay and jammer selection for secure two-way relay networks," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, pp. 310–320, 2012.

[63] S. Sharma, S. D. Roy, and S. Kundu, "Two way secure communication with two half-duplex DF relay," in *TENCON Region 10 Conference*. IEEE, 2017, pp. 869–874.

[64] C. Dang, L. J. Rodríguez, N. H. Tran, S. Shelly, and S. Sastry, "Secrecy capacity of the full-duplex AF relay wire-tap channel under residual self-interference," in *Wireless Communications and Networking Conference (WCNC)*. IEEE, 2015, pp. 99–104.

[65] L. Elsaid, M. Ranjbar, N. Raymondi, D. Nguyen, N. Tran, and A. Mahamadi, "Full-Duplex Decode-and-Forward Relaying: Secrecy Rates and Optimal Power Allocation," in *Vehicular Technology Conference (VTC Spring)*. IEEE, 2017, pp. 1–6.

[66] X. Hu, P. Mu, B. Wang, and Z. Li, "On the secrecy rate maximization with uncoordinated cooperative jamming by single-antenna helpers," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 5, pp. 4457–4462, 2017.

[67] K. Cao, Y. Cai, Y. Wu, and W. Yang, "Cooperative Jamming for Secure Communication With Finite Alphabet Inputs," *IEEE Communications Letters*, vol. 21, no. 9, pp. 2025–2028, 2017.

[68] H. Long, W. Xiang, J. Wang, Y. Zhang, and W. Wang, "Cooperative jamming and power allocation in three-phase two-way relaying wiretap systems," in *Wireless Communications and Networking Conference (WCNC)*. IEEE, 2013, pp. 4175–4179.

[69] Y. Oohama, "Capacity theorems for relay channels with confidential messages," in *International Symposium on Information Theory*. IEEE, 2007, pp. 926–930.

[70] X. He and A. Yener, "Cooperation with an untrusted relay: A secrecy perspective," *IEEE Transactions on Information Theory*, vol. 56, no. 8, pp. 3807–3827, 2010.

[71] M. Atallah and G. Kaddoum, "Secrecy analysis of cooperative network with untrustworthy relays using location-based multicasting technique," in *International Conference on Future Internet of Things and Cloud: Workshops (W-FiCloud)*. IEEE, 2017, pp. 206–210.

[72] L. Lv, J. Chen, L. Yang, and Y. Kuo, "Improving physical layer security in untrusted relay networks: cooperative jamming and power allocation," *IET Communications*, vol. 11, no. 3, pp. 393–399, 2017.

[73] S. Zhang, L. Fan, M. Peng, and H. V. Poor, "Near-optimal modulo-and-forward scheme for the untrusted relay channel," *IEEE Transactions on Information Theory*, vol. 62, no. 5, pp. 2545–2556, 2016.

[74] J. Xiong, L. Cheng, D. Ma, and J. Wei, "Destination-aided cooperative jamming for dual-hop amplify-and-forward MIMO untrusted relay systems," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 9, pp. 7274–7284, 2016.

[75] G. Luo, J. Li, Z. Liu, X. Tao, and F. Yang, "Physical Layer Security with Untrusted Relays in Wireless Cooperative Networks," in *Wireless Communications and Networking Conference (WCNC)*. IEEE, 2017, pp. 1–6.

[76] A. A. Zewail and A. Yener, "Two-Hop Untrusted Relay Channel with an External Eavesdropper Under Layered Secrecy Constraints," in *Global Communications Conference (GLOBECOM)*. IEEE, 2016, pp. 1–6.

[77] J.-B. Kim, J. Lim, and J. M. Cioffi, "Capacity scaling and diversity order for secure cooperative relaying with untrustworthy relays," *IEEE Transactions on Wireless Communications*, vol. 14, no. 7, pp. 3866–3876, 2015.

[78] J. Y. Ryu, J. Lee, and T. Q. Quek, "Trust degree-based cooperative transmission for communication secrecy," in *Global Communications Conference (GLOBECOM)*. IEEE, 2015, pp. 1–6.

[79] X. He and A. Yener, "End-to-end secure multi-hop communication with untrusted relays," *IEEE transactions on wireless communications*, vol. 12, no. 1, pp. 1–11, 2013.

[80] C. Jeong, I.-M. Kim, and D. I. Kim, "Joint secure beamforming design at the source and the relay for an amplify-and-forward MIMO untrusted relay system," *IEEE Transactions on Signal Processing*, vol. 60, no. 1, pp. 310–325, 2012.

[81] M. Kaliszan, J. Mohammadi, and S. Stanczak, "Cross-layer security in two-hop wireless Gaussian relay network with untrusted relays," in *International Conference on Communications (ICC)*. IEEE, 2013, pp. 2199–2204.

[82] R. F. Wyrembelski, A. Sezgin, and H. Boche, "Secrecy in broadcast channels with receiver side information," in *Conference on Signals, Systems and Computers (ASILOMAR)*. IEEE, 2011, pp. 290–294.

[83] X. He and A. Yener, "Two-hop secure communication using an untrusted relay," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, no. 1, p. 305146, 2009.

[84] ——, "Strong secrecy and reliable byzantine detection in the presence of an untrusted relay," *IEEE Transactions on Information Theory*, vol. 59, no. 1, pp. 177–192, 2013.

[85] C. Ling, L. Luzzi, J.-C. Belfiore, and D. Stehlé, "Semantically secure lattice codes for the gaussian wiretap channel," *IEEE Transactions on Information Theory*, vol. 60, no. 10, pp. 6399–6416, 2014.

[86] J. Richter, C. Scheunert, S. Engelmann, and E. A. Jorswieck, "Weak secrecy in the multiway untrusted relay channel with compute-and-forward," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 6, pp. 1262–1273, 2015.

[87] L. Sun, T. Zhang, Y. Li, and H. Niu, "Performance study of two-hop amplify-and-forward systems with untrustworthy relay nodes," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 8, pp. 3801–3807, 2012.

[88] J. Huang and A. L. Swindlehurst, "Joint transmit design and node selection for one-way and two-way untrusted relay channels," in *Asilomar Conference on Signals, Systems and Computers*. IEEE, 2013, pp. 1555–1559.

[89] D. Deng, X. Li, L. Fan, W. Zhou, R. Qingyang Hu, and Z. Zhou, "Secrecy Analysis of Multiuser Untrusted Amplify-and-Forward Relay Networks," *Wireless Communications and Mobile Computing*, vol. 2017, 2017.

[90] J. Mo, M. Tao, Y. Liu, B. Xia, and X. Ma, "Secure beamforming for MIMO two-way transmission with an untrusted relay," in *Wireless Communications and Networking Conference (WCNC)*. IEEE, 2013, pp. 4180–4185.

[91] F. Ding, H. Wang, S. Zhang, and M. Dai, "Multiuser untrusted relay networks with joint cooperative jamming and opportunistic scheduling under perfect and outdated csi," *Electronics Letters*, vol. 52, no. 23, pp. 1925–1927, 2016.

[92] A. A. Zewail and A. Yener, "Multi-Terminal Two-Hop Untrusted-Relay Networks with Hierarchical Security Guarantees," *IEEE Transactions on Information Forensics and Security*, 2017.

[93] L. Lai and H. El Gamal, "The relay–eavesdropper channel: Cooperation for secrecy," *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 4005–4019, 2008.

[94] E. Ekrem and S. Ulukus, "Secrecy in cooperative relay broadcast channels," *IEEE Transactions on Information Theory*, vol. 57, no. 1, pp. 137–155, 2011.

[95] S. Luo, J. Li, and A. Petropulu, "Physical layer security with uncoordinated helpers implementing cooperative jamming," in *Sensor Array and Multichannel Signal Processing Workshop (SAM)*. IEEE, 2012, pp. 97–100.

[96] X. Chen, L. Lei, H. Zhang, and C. Yuen, "Large-scale MIMO relaying techniques for physical layer security: AF or DF?" *IEEE Transactions on Wireless Communications*, vol. 14, no. 9, pp. 5135–5146, 2015.

[97] J. Li, A. P. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Transactions on Signal Processing*, vol. 59, no. 10, pp. 4985–4997, 2011.

[98] M. Jilani and T. Ohtsuki, "Joint SVD-GSVD precoding technique and secrecy capacity lower bound for the MIMO relay wire-tap channel," *EURASIP Journal on Wireless Communications and Networking*, vol. 2012, no. 1, p. 361, 2012.

[99] Z. Lin, Y. Cai, W. Yang, and L. Wang, "Robust secure switching transmission in multi-antenna relaying systems: cooperative jamming or decode-and-forward beamforming," *IET Communications*, vol. 10, no. 13, pp. 1673–1681, 2016.

[100] K. Eshteiwi, G. Kaddoum, and F. Gagnon, "Impact of imperfect channel estimation error and jamming on the performance of decode-and-forward relaying," in *International Conference on Ubiquitous Wireless Broadband (ICUWB)*. IEEE, 2015, pp. 1–5.

[101] Y. Yang, Q. Li, W.-K. Ma, J. Ge, and P. Ching, "Cooperative secure beamforming for AF relay networks with multiple eavesdroppers," *IEEE Signal Processing Letters*, vol. 20, no. 1, pp. 35–38, 2013.

[102] X. Wang, K. Wang, and X.-D. Zhang, "Secure relay beamforming with imperfect channel side information," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 5, pp. 2140–2155, 2013.

[103] M. Mirzaee and S. Akhlaghi, "The achievable secrecy rate of multi-antenna AF relaying using joint transmit and receive beamforming," in *International Symposium on Telecommunications (IST)*. IEEE, 2014, pp. 1122–1127.

[104] H.-M. Wang, F. Liu, and X.-G. Xia, "Joint source-relay precoding and power allocation for secure amplify-and-forward MIMO relay networks," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 8, pp. 1240–1250, 2014.

[105] C. Dang, L. Jiménez-Rodríguez, N. H. Tran, S. Shetty, and S. Sastry, "On Secrecy Rate and Optimal Power Allocation of the Full-Duplex Amplify-and-Forward Relay Wire-Tap Channel," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 5, pp. 3887–3899, 2017.

[106] Z. H. Awan, A. Zaidi, and L. Vandendorpe, "Secure communication over parallel relay channel," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 359–371, 2012.

[107] C. Cai, Y. Cai, X. Zhou, W. Yang, and W. Yang, "When does relay transmission give a more secure connection in wireless ad hoc networks?" *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 4, pp. 624–632, 2014.

[108] Y. Zou, X. Wang, W. Shen, and L. Hanzo, "Security versus reliability analysis of opportunistic relaying," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 6, pp. 2653–2661, 2014.

[109] D. W. K. Ng, E. S. Lo, and R. Schober, "Secure resource allocation and scheduling for OFDMA decode-and-forward relay networks," *IEEE Transactions on Wireless Communications*, vol. 10, no. 10, pp. 3528–3540, 2011.

[110] F. Jameel, S. Wyne, and Z. Ding, "Secure Communications in Three-Step Two-Way Energy Harvesting DF Relaying," *IEEE Communications Letters*, vol. 22, no. 2, pp. 308–311, Feb 2018.

[111] D. Goeckel, S. Vasudevan, D. Towsley, S. Adams, Z. Ding, and K. Leung, "Artificial noise generation from cooperative relays for everlasting secrecy in two-hop wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 10, pp. 2067–2076, 2011.

[112] R. F. Wyrembelski and H. Boche, "Physical layer integration of private, common, and confidential messages in bidirectional relay networks," *IEEE Transactions on Wireless Communications*, vol. 11, no. 9, pp. 3170–3179, 2012.

[113] T. Wang, L. Song, Z. Han, X. Cheng, and B. Jiao, "Power allocation using vickrey auction and sequential first-price auction games for physical layer security in cognitive relay networks," in *International Conference on Communications (ICC)*. IEEE, 2012, pp. 1683–1687.

[114] K. Guan, E. C. Song, E. Soljanin, P. J. Winzer, and A. M. Tulino, "Physical layer security in space-division multiplexed fiber optic communications," in *Signals, Systems and Computers (ASILOMAR), 2012 Conference Record of the Forty Sixth Asilomar Conference on*. IEEE, 2012, pp. 654–658.

[115] Z. Ding, M. Xu, J. Lu, and F. Liu, "Improving wireless security for bidirectional communication scenarios," *IEEE Transactions on vehicular technology*, vol. 61, no. 6, pp. 2842–2848, 2012.

[116] Y. Yang, C. Sun, H. Zhao, H. Long, and W. Wang, "Algorithms for secrecy guarantee with null space beamforming in two-way relay networks," *IEEE transactions on signal processing*, vol. 62, no. 8, pp. 2111–2126, 2014.

[117] B. Han, J. Li, J. Su, M. Guo, and B. Zhao, "Secrecy capacity optimization via cooperative relaying and jamming for WANETs," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 4, pp. 1117–1128, 2015.

[118] H. Ju, D. Kim, H. V. Poor, and D. Hong, "Bi-directional beamforming and its capacity scaling in pairwise two-way communications," *IEEE Transactions on Wireless Communications*, vol. 11, no. 1, pp. 346–357, 2012.

[119] H. Ju, X. Shang, H. V. Poor, and D. Hong, "Bi-directional use of spatial resources and effects of spatial correlation," *IEEE Transactions on Wireless Communications*, vol. 10, no. 10, pp. 3368–3379, 2011.

[120] H. Ju, E. Oh, and D. Hong, "Catching resource-devouring worms in next-generation wireless relay systems: Two-way relay and full-duplex relay," *IEEE Communications Magazine*, vol. 47, no. 9, 2009.

[121] D. Kim, S. Park, H. Ju, and D. Hong, "Transmission capacity of full-duplex-based two-way ad hoc networks with ARQ protocol," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 7, pp. 3167–3183, 2014.

[122] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Transactions on Signal Processing*, vol. 61, no. 20, pp. 4962–4974, 2013.

[123] O. Cepheli, S. Tedik, and G. K. Kurt, "A high data rate wireless communication system with improved secrecy: Full duplex beamforming," *IEEE communications letters*, vol. 18, no. 6, pp. 1075–1078, 2014.

[124] D. Kim, H. Lee, and D. Hong, "A survey of in-band full-duplex transmission: From the perspective of PHY and MAC layers," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2017–2046, 2015.

[125] M. Hui and M. Piming, "Convex analysis based beamforming of decode-and-forward cooperation for improving wireless physical layer security," in *Advanced Communication Technology (ICACT), 2012 14th International Conference on*. IEEE, 2012, pp. 754–758.

[126] S. Huang, J. Tan, and J. Xu, "Nash Bargaining Game Based Subcarrier Allocation for Physical Layer Security in Orthogonal Frequency Division Multiplexing System," in *International Conference on Ubiquitous Intelligence and Computing - Autonomic and Trusted Computing and Scalable Computing and Communications Workshops (UIC-ATC-ScalCom)*. IEEE, 2015, pp. 1094–1100.

[127] Z. E. Ankaralı, M. H. Yılmaz, M. Hafez, and H. Arslan, "Channel independent physical layer security," in *Annual Wireless and Microwave Technology Conference (WAMICON)*. IEEE, 2016, pp. 1–5.

[128] W. Aman, G. A. S. Sidhu, T. Jabeen, F. Gao, and S. Jin, "Enhancing physical layer security in dual-hop multiuser transmission," in *Wireless Communications and Networking Conference (WCNC)*. IEEE, 2016, pp. 1–6.

[129] Y. Zou, X. Wang, and W. Shen, "Intercept probability analysis of cooperative wireless networks with best relay selection in the presence of eavesdropping attack," in *International Conference on Communications (ICC)*. IEEE, 2013, pp. 2183–2187.

[130] J. Huang and A. L. Swindlehurst, "Wireless physical layer security enhancement with buffer-aided relaying," in *Asilomar Conference on Signals, Systems and Computers*. IEEE, 2013, pp. 1560–1564.

[131] L. Chen, "Physical layer security for cooperative relaying in broadcast networks," in *MILITARY COMMUNICATIONS CONFERENCE (MILCOM)*. IEEE, 2011, pp. 91–96.

[132] L. Fan, X. Lei, N. Yang, T. Q. Duong, and G. K. Karagiannidis, "Secrecy cooperative networks with outdated relay selection over correlated fading channels," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 8, pp. 7599–7603, 2017.

[133] M. F. Haroun and T. A. Gulliver, "Secret key generation using chaotic signals over frequency selective fading channels," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 8, pp. 1764–1775, 2015.

[134] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Amplify-and-forward based cooperation for secure wireless communications," in *International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2009, pp. 2613–2616.

[135] H. Hui, A. L. Swindlehurst, G. Li, and J. Liang, "Secure relay and jammer selection for physical layer security," *IEEE Signal Processing Letters*, vol. 22, no. 8, pp. 1147–1151, 2015.

[136] C. Kundu, S. Ghose, and R. Bose, "Secrecy outage of dual-hop regenerative multi-relay system with relay selection," *IEEE Transactions on Wireless Communications*, vol. 14, no. 8, pp. 4614–4625, 2015.

[137] S. Ghose, C. Kundu, and R. Bose, "Secrecy performance of dual-hop decode-and-forward relay system with diversity combining at the eavesdropper," *IET Communications*, vol. 10, no. 8, pp. 904–914, 2016.

[138] F. S. Al-Qahtani, C. Zhong, and H. M. Alnuweiri, "Opportunistic relay selection for secrecy enhancement in cooperative networks," *IEEE Transactions on Communications*, vol. 63, no. 5, pp. 1756–1770, 2015.

[139] C. Kundu, T. M. Ngatched, and O. A. Dobre, "Secrecy Performance of Dual-Hop Threshold Relaying System with Diversity Reception," in *Vehicular Technology Conference (VTC-Fall)*. IEEE, 2016, pp. 1–6.

[140] M. R. Khandaker, K.-K. Wong, and G. Zheng, "Truth-Telling Mechanism for Two-Way Relay Selection for Secrecy Communications With Energy-Harvesting Revenue," *IEEE Transactions on Wireless Communications*, vol. 16, no. 5, pp. 3111–3123, 2017.

[141] A. H. A. El-Malek, A. M. Salhab, S. A. Zummo, and M.-S. Alouini, "Security-reliability trade-off analysis for multiuser SIMO mixed RF/FSO relay networks with opportunistic user scheduling," *IEEE Transactions on Wireless Communications*, vol. 15, no. 9, pp. 5904–5918, 2016.

[142] X. Lei, L. Fan, R. Q. Hu, D. S. Michalopoulos, and P. Fan, "Secure multiuser communications in multiple decode-and-forward relay networks with direct links," in *Global Communications Conference (GLOBECOM)*. IEEE, 2014, pp. 3180–3185.

[143] L. Fan, N. Yang, T. Q. Duong, M. Elkashlan, and G. K. Karagiannidis, "Exploiting direct links for physical layer security in multiuser multirelay networks," *IEEE Transactions on Wireless Communications*, vol. 15, no. 6, pp. 3856–3867, 2016.

[144] K. Shim, N. T. Do, and B. An, "Performance analysis of physical layer security of opportunistic scheduling in multiuser multirelay cooperative networks," *Sensors*, vol. 17, no. 2, p. 377, 2017.

[145] R. F. Wyrembelski, M. Wiese, and H. Boche, "Strong secrecy in bidirectional broadcast channels with confidential messages," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 2, pp. 324–334, 2013.

[146] V. N. Q. Bao, N. Linh-Trung, and M. Debbah, "Relay selection schemes for dual-hop networks under security constraints with multiple eavesdroppers," *IEEE transactions on wireless communications*, vol. 12, no. 12, pp. 6076–6085, 2013.

[147] M. Yang, D. Guo, Y. Huang, T. Q. Duong, and B. Zhang, "Secure multiuser scheduling in downlink dual-hop regenerative relay networks over nakagami-m fading channels," *IEEE Transactions on Wireless Communications*, vol. 15, no. 12, pp. 8009–8024, 2016.

[148] R. Bassily and S. Ulukus, "Secure communication in multiple relay networks through decode-and-forward strategies," *Journal of Communications and Networks*, vol. 14, no. 4, pp. 352–363, 2012.

[149] G. Kramer, M. Gastpar, and P. Gupta, "Cooperative strategies and capacity theorems for relay networks," *IEEE Transactions on Information Theory*, vol. 51, no. 9, pp. 3037–3063, 2005.

[150] P. Gupta and P. Kumar, "Towards an information theory of large networks: An achievable rate region," *IEEE Transactions on Information Theory*, vol. 49, no. 8, pp. 1877–1894, 2003.

[151] J. Y. Ryu, J. Lee, and T. Q. Quek, "Confidential Cooperative Communication With Trust Degree of Potential Eavesdroppers," *IEEE Transactions on Wireless Communications*, vol. 15, no. 6, pp. 3823–3836, 2016.

[152] J. Li, R. Li, and J. Kato, "Future trust management framework for mobile ad hoc networks," *IEEE Communications Magazine*, vol. 46, no. 4, 2008.

[153] Y. L. Sun, Z. Han, W. Yu, and K. R. Liu, "A trust evaluation framework in distributed networks: Vulnerability analysis and defense against attacks," in *International Conference on Computer Communications*. IEEE, 2006, pp. 1–13.

[154] B. Bloessl, M. Gerla, and F. Dressler, "Ieee802. 11p in fast fading scenarios: from traces to comparative studies of receive algorithms," in *Proceedings of the First ACM International Workshop on Smart, Autonomous, and Connected Vehicular Systems and Services*. ACM, 2016, pp. 1–5.

[155] F. Jameel, M. A. A. Haider, A. A. Butt *et al.*, "Performance analysis of VANETs under Rayleigh, Rician, Nakagami-m and Weibull fading," in *International Conference on Communication, Computing and Digital Systems (C-CODE)*. IEEE, 2017, pp. 127–132.

[156] I. Bekmezci, O. K. Sahingoz, and Ş. Temel, "Flying ad-hoc networks (FANETs): A survey," *Ad Hoc Networks*, vol. 11, no. 3, pp. 1254–1270, 2013.

[157] J. Wang, C. Jiang, Z. Han, Y. Ren, R. G. Maunder, and L. Hanzo, "Cooperative distributed unmanned aerial vehicular networks: Small and mini drones," *IEEE Vehicular Technology Magazine*, pp. 1–18, 2016.

[158] L. Wang, Y. Cai, Y. Zou, W. Yang, and L. Hanzo, "Joint relay and jammer selection improves the physical layer security in the face of CSI feedback delays," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 8, pp. 6259–6274, 2016.

[159] Y. Zou and J. Zhu, "Joint Relay and Jammer Selection for Wireless Physical-Layer Security," in *Physical-Layer Security for Cooperative Relay Networks*. Springer, 2016, pp. 35–52.

[160] L. Wang, T. Ke, M. Song, Y. Wei, and Y. Teng, "Research on secrecy capacity oriented relay selection for mobile cooperative networks," in *International Conference on Cloud Computing and Intelligence Systems (CCIS)*. IEEE, 2011, pp. 443–447.

[161] X. Cao, J. Zhang, L. Fu, W. Wu, and X. Wang, "Optimal secrecy capacity-delay tradeoff in large-scale mobile ad hoc networks," *IEEE/ACM Transactions on Networking*, vol. 24, no. 2, pp. 1139–1152, 2016.

[162] Q. Wang, Z. Chen, W. Mei, and J. Fang, "Improving physical layer security using UAV-enabled mobile relaying," *IEEE Wireless Communications Letters*, 2017.

[163] M. Yang, B. Zhang, Y. Huang, D. Guo, and H. Yang, "Secrecy outage analysis of cooperative relay system with multiuser scheduling," in *International Symposium on Communications and Information Technologies (ISCIT)*. IEEE, 2016, pp. 38–43.

[164] X. Gong, C. T. Ps, J. Zhang, and H. V. Poor, "Opportunistic cooperative networking: To relay or not to relay?" *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 2, pp. 307–314, 2012.

[165] J. Zhu, D. W. K. Ng, N. Wang, R. Schober, and V. K. Bhargava, "Analysis and design of secure massive MIMO systems in the presence of hardware impairments," *IEEE Transactions on Wireless Communications*, vol. 16, no. 3, pp. 2001–2016, 2017.

[166] D. T. Hung, T. T. Duy, D. Q. Trinh, V. N. Q. Bao, and T. Hanhv, "Impact of hardware impairments on secrecy performance of multi-hop relay networks in presence of multiple eavesdroppers," in *National Foundation for Science and Technology Development Conference on Information and Computer Science (NICS)*. IEEE, 2016, pp. 113–118.

[167] L. G. Thien, P. T. Tin, T. T. Nhat, T. T. Duy, and M. Voznak, "Performance evaluation of multi-hop cooperative transmission protocol with hardware noises and presence of eavesdropper," in *International Conference on System Science and Engineering (ICSSE)*. IEEE, 2017, pp. 244–248.

[168] S. Q. Nguyen and H. Y. Kong, "Secrecy enhancement in two-hop DF relaying system under hardware impairment," *International Journal of Electronics*, vol. 104, no. 3, pp. 442–461, 2017.

[169] T. T. Tran and H. Y. Kong, "CSI-secured orthogonal jamming method for wireless physical layer security," *IEEE Communications Letters*, vol. 18, no. 5, pp. 841–844, 2014.

[170] I. Krikidis, "Opportunistic relay selection for cooperative networks with secrecy constraints," *IET communications*, vol. 4, no. 15, pp. 1787–1791, 2010.

[171] Y. Tang, J. Xiong, D. Ma, and X. Zhang, "Robust artificial noise aided transmit design for MISO wiretap channels with channel uncertainty," *IEEE Communications Letters*, vol. 17, no. 11, pp. 2096–2099, 2013.

[172] W. Li, M. Ghogho, B. Chen, and C. Xiong, "Secure communication via sending artificial noise by the receiver: Outage secrecy capacity/region analysis," *IEEE Communications Letters*, vol. 16, no. 10, pp. 1628–1631, 2012.

[173] S.-H. L. Tsai and H. V. Poor, "Power allocation for artificial-noise secure MIMO precoding systems," *Power*, vol. 1, 2014.

[174] X. Zhang, M. R. McKay, X. Zhou, and R. W. Heath, "Artificial-noise-aided secure multi-antenna transmission with limited feedback," *IEEE Transactions on Wireless Communications*, vol. 14, no. 5, pp. 2742–2754, 2015.

[175] J. Yang, I.-M. Kim, and D. I. Kim, "Power-constrained optimal cooperative jamming for multiuser broadcast channel," *IEEE Wireless Communications Letters*, vol. 2, no. 4, pp. 411–414, 2013.

[176] Z. Han, N. Marina, M. Debbah, and A. Hjørungnes, "Physical layer security game: interaction between source, eavesdropper, and friendly jammer," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, no. 1, p. 452907, 2010.

[177] Y. Yao, W. Zhou, B. Kou, and Y. Wang, "Dynamic Spectrum Access With Physical Layer Security: A Game-Based Jamming Approach," *IEEE Access*, vol. 6, pp. 12 052–12 059, 2018.

[178] Q. Li and W.-K. Ma, "Spatially selective artificial-noise aided transmit optimization for MISO multi-eves secrecy rate maximization," *IEEE Transactions on Signal Processing*, vol. 61, no. 10, pp. 2704–2717, 2013.

[179] J. K. Tugnait, "Using artificial noise to improve detection performance for wireless user authentication in time-variant channels," *IEEE Wireless Communications Letters*, vol. 3, no. 4, pp. 377–380, 2014.

[180] D. H. Ibrahim, E. S. Hassan, and S. A. El-Dolil, "Improving physical layer security in two-way cooperative networks with multiple eavesdroppers," in *International Conference on Informatics and Systems (INFOS)*. IEEE, 2014, pp. ORDS–8.

[181] A. Mukherjee and A. L. Swindlehurst, "Jamming games in the MIMO wiretap channel with an active eavesdropper," *IEEE Transactions on Signal Processing*, vol. 61, no. 1, pp. 82–91, 2013.

[182] Z. Chu, K. Cumanan, Z. Ding, M. Johnston, and S. Y. Le Goff, "Secrecy rate optimizations for a MIMO secrecy channel with a cooperative jammer," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 5, pp. 1833–1847, 2015.

[183] S. Huang, L. Zhu, and S. Liu, "Based on virtual beamforming cooperative jamming with Stackelberg game for physical layer security in the heterogeneous wireless network," *EURASIP Journal on Wireless Communications and Networking*, vol. 2018, no. 1, p. 69, 2018.

[184] S. Kakkar, I. S. Makkar, and A. Mohapatra, "Secret key generation using OFDM samples," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 18, no. 4, pp. 439–454, 2015.

[185] D. Steinmetzer, M. Schulz, and M. Hollick, "Lockpicking physical layer key exchange: Weak adversary models invite the thief," in *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*. ACM, 2015, p. 1.

[186] Q. Li, Y. Yang, W.-K. Ma, M. Lin, J. Ge, and J. Lin, "Robust cooperative beamforming and artificial noise design for physical-layer secrecy in af multi-antenna multi-relay networks," *IEEE Transactions on Signal Processing*, vol. 63, no. 1, pp. 206–220, 2015.

[187] N. Li, X. Tao, and J. Xu, "Artificial noise assisted communication in the multiuser downlink: optimal power allocation," *IEEE communications letters*, vol. 19, no. 2, pp. 295–298, 2015.

[188] N. Romero-Zurita, D. McLernon, M. Ghogho, and A. Swami, "PHY layer security based on protected zone and artificial noise," *IEEE Signal Processing Letters*, vol. 20, no. 5, pp. 487–490, 2013.

[189] N. Romero-Zurita, D. McLernon, and M. Ghogho, "Physical layer security by robust masked beamforming and protected zone optimisation," *IET Communications*, vol. 8, no. 8, pp. 1248–1257, 2014.

[190] M. A. Kishk and H. Dhillon, "Stochastic geometry-based comparison of secrecy enhancement techniques in D2D networks," *IEEE Wireless Communications Letters*, 2017.

[191] Y. Huo, Y. Tian, L. Ma, X. Cheng, and T. Jing, "Jamming Strategies for Physical Layer Security," *IEEE Wireless Communications*, vol. 25, no. 1, pp. 148–153, 2018.

[192] J. Huang and A. L. Swindlehurst, "Cooperation strategies for secrecy in mimo relay networks with unknown eavesdropper CSI," in *International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2011, pp. 3424–3427.

[193] L. Wang and H. Wu, "Jamming partner selection for maximising the worst D2D secrecy rate based on social trust," *Transactions on Emerging Telecommunications Technologies*, vol. 28, no. 2, 2017.

[194] J. H. Lee and W. Choi, "Multiuser diversity for secrecy communications using opportunistic jammer selection: Secure DoF and jammer scaling law," *IEEE Transactions on Signal Processing*, vol. 62, no. 4, pp. 828–839, 2014.

[195] F. Jiang, C. Zhu, J. Peng, W. Liu, Z. Zhu, and Y. He, "Joint relay and jammer selection and power control for physical layer security in two-way relay networks with imperfect CSI," *Wireless Personal Communications*, vol. 85, no. 3, pp. 841–862, 2015.

[196] S. Soderi, L. Mucchi, M. Hämäläinen, A. Piva, and J. Iinatti, "Physical layer security based on spread-spectrum watermarking and jamming receiver," *Transactions on Emerging Telecommunications Technologies*, vol. 28, no. 7, 2017.

[197] S. Gollakota and D. Katabi, "Physical layer wireless security made fast and channel independent," in *Proceedings of IEEE INFOCOM*. IEEE, 2011, pp. 1125–1133.

[198] C. Zhang and J. Ge, "Partial Jamming for Secure Two-Way Relay Systems Without Wiretap Information: One < Two," *Wireless Personal Communications*, vol. 95, no. 4, pp. 4013–4024, 2017.

[199] W. Fang, F. Li, Y. Sun, L. Shan, S. Chen, C. Chen, and M. Li, "Information Security of PHY Layer in Wireless Networks," *Journal of Sensors*, vol. 2016, 2016.

[200] J. Xie and S. Ulukus, "Secure degrees of freedom of the Gaussian wiretap channel with helpers and no eavesdropper CSI: Blind cooperative jamming," in *Annual Conference on Information Sciences and Systems (CISS)*. IEEE, 2013, pp. 1–5.

[201] X. Jianwei and S. Ulukus, "Secure degrees of freedom of one-hop wireless networks," *IEEE Transactions on Information Theory*, vol. 60, no. 6, pp. 3359–3378, 2014.

[202] H. Wang, X. Zhou, and M. C. Reed, "Physical layer security in cellular networks: A stochastic geometry approach," *IEEE Transactions on Wireless Communications*, vol. 12, no. 6, pp. 2776–2787, 2013.

[203] S. Marano and V. Matta, "Achieving perfect secrecy by pdf-bandlimited jamming," *IEEE Signal Processing Letters*, vol. 21, no. 1, pp. 83–87, 2014.

[204] L. Zhou, D. Wu, B. Zheng, and M. Guizani, "Joint physical-application layer security for wireless multimedia delivery," *IEEE Communications Magazine*, vol. 52, no. 3, pp. 66–72, 2014.

[205] X.-y. Li, L. Jin, and K.-z. Huang, "A physical layer security transmission mechanism based on joint channel characteristics in relay system," in *International Conference on Communication Technology (ICCT)*. IEEE, 2012, pp. 599–603.

[206] B. Yang, W. Wang, B. Yao, and Q. Yin, "Destination assisted secret wireless communication with cooperative helpers," *IEEE Signal Processing Letters*, vol. 20, no. 11, pp. 1030–1033, 2013.

[207] Y. Liu, A. P. Petropulu, and H. V. Poor, "Joint decode-and-forward and jamming for wireless physical layer security with destination assistance," in *Conference Record of the Forty Fifth Asilomar Conference on Signals, Systems and Computers (ASILOMAR)*. IEEE, 2011, pp. 109–113.

[208] Y. Liu and A. P. Petropulu, "Relay selection and scaling law in destination assisted physical layer secrecy systems," in *Statistical Signal Processing Workshop (SSP)*. IEEE, 2012, pp. 381–384.

[209] ——, "Destination assisted cooperative jamming for wireless physical layer security," in *International Workshop on Information Forensics and Security (WIFS)*. IEEE, 2012, pp. 282–287.

[210] S. Luo, J. Li, and A. P. Petropulu, "Uncoordinated cooperative jamming for secret communications," *IEEE transactions on information forensics and security*, vol. 8, no. 7, pp. 1081–1090, 2013.

[211] S. Luo, J. Li, and A. Petropulu, "Outage constrained secrecy rate maximization using cooperative jamming," in *Statistical Signal Processing Workshop (SSP), 2012 IEEE*. IEEE, 2012, pp. 389–392.

[212] R. Zhao, Y. Huang, W. Wang, and V. K. Lau, "Ergodic achievable secrecy rate of multiple-antenna relay systems with cooperative jamming," *IEEE Transactions on Wireless Communications*, vol. 15, no. 4, pp. 2537–2551, 2016.

[213] N. Kolokotronis, K. Fytrakis, A. Katsiotis, and N. Kalouptsidis, "A cooperative jamming protocol for physical layer security in wireless networks," in *Acoustics, Speech and Signal Processing (ICASSP), 2015 IEEE International Conference on*. IEEE, 2015, pp. 5803–5807.

[214] I. Stanojev and A. Yener, "Improving secrecy rate via spectrum leasing for friendly jamming," *IEEE Transactions on Wireless Communications*, vol. 12, no. 1, pp. 134–145, 2013.

[215] N. Ouyang, X.-Q. Jiang, E. Bai, and H.-M. Wang, "Destination Assisted Jamming and Beamforming for Improving the Security of AF Relay Systems," *IEEE Access*, vol. 5, pp. 4125–4131, 2017.

[216] S. Jia, J. Zhang, H. Zhao, and R. Zhang, "Destination Assisted Secret Transmission in Wireless Relay Networks," in *Vehicular Technology Conference (VTC-Fall)*. IEEE, 2016, pp. 1–5.

[217] N. Kolokotronis and M. Athanasakos, "Improving physical layer security in DF relay networks via two-stage cooperative jamming," in *Signal Processing Conference (EUSIPCO), 2016 24th European*. IEEE, 2016, pp. 1173–1177.

[218] J. Liu, Z. Liu, Y. Zeng, and J. Ma, "Cooperative Jammer Placement for Physical Layer Security Enhancement," *IEEE Network*, vol. 30, no. 6, pp. 56–61, 2016.

[219] A. Bakhtiar, N. Zamir, N. Soon Xin, and M. F. U. Butt, "Distributed Matching Algorithms: Maximizing Secrecy in the Presence of Untrusted Relay," *Radioengineering*, vol. 26, no. 2, p. 601, 2017.

[220] L. Huang, X. Fan, Y. Huo, C. Hu, Y. Tian, and J. Qian, "A Novel Cooperative Jamming Scheme for Wireless Social Networks Without Known CSI," *IEEE Access*, vol. 5, pp. 26 476–26 486, 2017.

[221] K. Wang, L. Yuan, T. Miyazaki, S. Guo, and Y. Sun, "Antieavesdropping With Selfish Jamming in Wireless Networks: A Bertrand Game Approach," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 7, pp. 6268–6279, 2017.

[222] Y. Shen and Y. Zhang, "Transmission protocol for secure big data in two-hop wireless networks with cooperative jamming," *Information Sciences*, vol. 281, pp. 201–210, 2014.

[223] Z. Liu, J. Liu, N. Kato, J. Ma, and Q. Huang, "Divide-and-conquer based cooperative jamming: Addressing multiple eavesdroppers in close proximity," in *International Conference on Computer Communications*. IEEE, 2016, pp. 1–9.

[224] X. Ding, T. Song, Y. Zou, and X. Chen, "Security-Reliability Tradeoff for Friendly Jammer Assisted User-Pair Selection in the Face of Multiple Eavesdroppers," *IEEE Access*, vol. 4, pp. 8386–8393, 2016.

[225] X. Feng, X. Gao, and R. Zong, "Cooperative jamming for enhancing security of cognitive radio networks with multiple primary users," *China Communications*, vol. 14, no. 7, pp. 1–15, 2017.

[226] L. Hu, H. Wen, B. Wu, J. Tang, F. Pan, and R.-F. Liao, "Cooperative Jamming Aided Secrecy Enhancement in Wireless Networks With Passive Eavesdroppers," *IEEE Transactions on Vehicular Technology*, 2017.

[227] K. Cumanan, G. C. Alexandropoulos, Z. Ding, and G. K. Karagiannidis, "Secure communications with cooperative jamming: Optimal power allocation and secrecy outage analysis," *IEEE Transactions on Vehicular Technology*, 2017.

[228] F.-S. Saeidi-Khabisi, V. T. Vakili, and D. Abbasi-Moghadam, "Improving the Physical Layer Security in Cooperative Networks with Multiple Eavesdroppers," *Wireless Personal Communications*, vol. 95, no. 3, pp. 3295–3320, 2017.

[229] M. Zhang, M. Ding, L. Gui, H. Luo, and M. Bennis, "Sum Secrecy Rate Maximization for Relay-Aided Multiple-Source Multiple-Destination Networks," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 5, pp. 4098–4109, 2017.

[230] Z. Ding, K. K. Leung, D. L. Goeckel, and D. Towsley, "On the application of cooperative transmission to secrecy communications," *IEEE journal on selected areas in communications*, vol. 30, no. 2, pp. 359–368, 2012.

[231] X. Zhou, M. Tao, and R. A. Kennedy, "Cooperative jamming for secrecy in decentralized wireless networks," in *International Conference on Communications (ICC)*. IEEE, 2012, pp. 2339–2344.

[232] Y. Wu, K. Guo, J. Huang, and X. S. Shen, "Secrecy-based energy-efficient data offloading via dual connectivity over unlicensed spectrums," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 12, pp. 3252–3270, 2016.

[233] J. P. Vilela, P. C. Pinto, and J. Barros, "Position-based jamming for enhanced wireless secrecy," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 616–627, 2011.

[234] R. Zhang, L. Song, Z. Han, and B. Jiao, "Physical layer security for two-way untrusted relaying with friendly jammers," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 8, pp. 3693–3704, 2012.

[235] A. Wang, Y. Cai, W. Yang, and Z. Hou, "A Stackelberg security game with cooperative jamming over a multiuser OFDMA network," in *Wireless Communications and Networking Conference (WCNC)*. IEEE, 2013, pp. 4169–4174.

[236] N. Zhang, N. Cheng, N. Lu, X. Zhang, J. W. Mark, and X. S. Shen, "Partner selection and incentive mechanism for physical layer security," *IEEE Transactions on Wireless Communications*, vol. 14, no. 8, pp. 4265–4276, 2015.

[237] D.-S. Shiu, G. J. Foschini, M. J. Gans, and J. M. Kahn, "Fading correlation and its effect on the capacity of multielement antenna systems," *IEEE Transactions on communications*, vol. 48, no. 3, pp. 502–513, 2000.

[238] R. Y. Mesleh, H. Haas, S. Sinanovic, C. W. Ahn, and S. Yun, "Spatial modulation," *IEEE Transactions on Vehicular Technology*, vol. 57, no. 4, pp. 2228–2241, 2008.

[239] H. Shin and J. H. Lee, "Capacity of multiple-antenna fading channels: Spatial fading correlation, double scattering, and keyhole," *IEEE Transactions on Information Theory*, vol. 49, no. 10, pp. 2636–2647, 2003.

[240] A. Goldsmith, S. A. Jafar, N. Jindal, and S. Vishwanath, "Capacity limits of mimo channels," *IEEE Journal on selected areas in Communications*, vol. 21, no. 5, pp. 684–702, 2003.

[241] Z. Rezki, A. Khisti, and M.-S. Alouini, "On the secrecy capacity of the wiretap channel with imperfect main channel estimation," *IEEE Transactions on Communications*, vol. 62, no. 10, pp. 3652–3664, 2014.

[242] J. M. Taylor, M. Hempel, H. Sharif, S. Ma, and Y. Yang, "Impact of channel estimation errors on effectiveness of eigenvector-based jamming for physical layer security in wireless networks," in *International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*. IEEE, 2011, pp. 122–126.

[243] S. Iwata, T. Ohtsuki, and P.-Y. Kam, "A Lower Bound on Secrecy Capacity for MIMO Wiretap Channel Aided by a Cooperative Jammer With Channel Estimation Error," *IEEE Access*, vol. 5, pp. 4636–4645, 2017.

[244] A. A. Nasir, H. D. Tuan, T. Q. Duong, and H. V. Poor, "Secrecy rate beamforming for multicell networks with information and energy harvesting," *IEEE Transactions on Signal Processing*, vol. 65, no. 3, pp. 677–689, 2017.

[245] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Physical layer network security in the full-duplex relay system," *IEEE transactions on information forensics and security*, vol. 10, no. 3, pp. 574–583, 2015.

[246] H. Deng, H.-M. Wang, W. Guo, and W. Wang, "Secrecy transmission with a helper: To relay or to jam," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 2, pp. 293–307, 2015.

[247] L. Tang, X. Gong, J. Wu, and J. Zhang, "Secure wireless communications via cooperative relaying and jamming," in *GLOBECOM Workshops (GC Wkshps)*. IEEE, 2011, pp. 849–853.

[248] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Transactions on Signal Processing*, vol. 59, no. 10, pp. 4871–4884, 2011.

[249] C. Wang, H.-M. Wang, and X.-G. Xia, "Hybrid opportunistic relaying and jamming with power allocation for secure cooperative networks," *IEEE Transactions on Wireless Communications*, vol. 14, no. 2, pp. 589–605, 2015.

[250] D. Wang, P. Ren, Q. Du, L. Sun, and Y. Wang, "Cooperative Relaying and Jamming for Primary Secure Communication in Cognitive Two-Way Networks," in *Vehicular Technology Conference (VTC Spring)*. IEEE, 2016, pp. 1–5.

[251] H. Zhang, H. Xing, J. Cheng, A. Nallanathan, and V. C. Leung, "Secure resource allocation for OFDMA two-way relay wireless sensor networks without and with cooperative jamming," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 5, pp. 1714–1725, 2016.

[252] Z. Lin, Y. Cai, W. Yang, and X. Xu, "Opportunistic relaying and jamming with robust design in hybrid full/half-duplex relay system," *EURASIP Journal on Wireless Communications and Networking*, vol. 2016, no. 1, p. 129, 2016.

[253] L. Yang, J. Chen, H. Jiang, S. A. Vorobyov, and H. Zhang, "Optimal Relay Selection for Secure Cooperative Communications With an Adaptive Eavesdropper," *IEEE Transactions on Wireless Communications*, vol. 16, no. 1, pp. 26–42, 2017.

[254] H. Guo, Z. Yang, L. Zhang, J. Zhu, and Y. Zou, "Power-Constrained Secrecy Rate Maximization for Joint Relay and Jammer Selection Assisted Wireless Networks," *IEEE Transactions on Communications*, vol. 65, no. 5, pp. 2180–2193, 2017.

[255] D. Wang, P. Ren, Q. Du, Y. Wang, and L. Sun, "Secure cooperative transmission against jamming-aided eavesdropper for ARQ based wireless networks," *IEEE Access*, vol. 5, pp. 3763–3776, 2017.

[256] C. Gu and C. Zhang, "Joint distributed beamforming and jamming schemes in decode-and-forward relay networks for physical layer secrecy," *EURASIP Journal on Wireless Communications and Networking*, vol. 2017, no. 1, p. 206, 2017.

[257] W. Lu, K. Gu, M. Jia, Z. Lu, and H. Peng, "Joint resource optimization for secure transmission in cooperative CR networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2017, no. 1, p. 193, 2017.

[258] L. Wang, M. Elkashlan, T. Q. Duong, and R. W. Heath, "Secure communication in cellular networks: The benefits of millimeter wave mobile broadband," in *International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*. IEEE, 2014, pp. 115–119.

[259] L. Sun, P. Ren, Q. Du, Y. Wang, and Z. Gao, "Security-aware relaying scheme for cooperative networks with untrusted relay nodes," *IEEE Communications Letters*, vol. 19, no. 3, pp. 463–466, 2015.

[260] M. Ju, D.-H. Kim, and K.-S. Hwang, "Opportunistic transmission of nonregenerative network with untrusted relay," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 6, pp. 2703–2709, 2015.

[261] Y. Liu, L. Li, and M. Pesavento, "Enhancing physical layer security in untrusted relay networks with artificial noise: A symbol error rate based approach," in *Sensor Array and Multichannel Signal Processing Workshop (SAM)*. IEEE, 2014, pp. 261–264.

[262] K.-H. Park and M.-S. Alouini, "Secure amplify-and-forward untrusted relaying networks using cooperative jamming and zero-forcing cancelation," in *Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*. IEEE, 2015, pp. 234–238.

[263] J. Huang, A. Mukherjee, and A. L. Swindlehurst, "Secure communication via an untrusted non-regenerative relay in fading channels," *IEEE Transactions on Signal Processing*, vol. 61, no. 10, pp. 2536–2550, 2013.

[264] H. Wu, X. Tao, Z. Han, N. Li, and J. Xu, "Secure Transmission in MISOME Wiretap Channel With Multiple Assisting Jammers: Maximum Secrecy Rate and Optimal Power Allocation," *IEEE Transactions on Communications*, vol. 65, no. 2, pp. 775–789, 2017.

[265] Z. Ding, Z. Ma, and P. Fan, "Asymptotic studies for the impact of antenna selection on secure two-way relaying communications with artificial noise," *IEEE Transactions on Wireless Communications*, vol. 13, no. 4, pp. 2189–2203, 2014.

[266] A. El Shafie, A. Mabrouk, K. Tourki, N. Al-Dhahir, and R. Hamila, "Securing Untrusted RF-EH Relay Networks Using Cooperative Jamming Signals," *IEEE Access*, vol. 5, pp. 24 353–24 367, 2017.

[267] D. H. Ibrahim, E. S. Hassan, and S. A. El-Dolil, "Relay and jammer selection schemes for improving physical layer security in two-way cooperative networks," *computers & security*, vol. 50, pp. 47–59, 2015.

[268] N.-E. Wu and H.-J. Li, "Effect of feedback delay on secure cooperative networks with joint relay and jammer selection," *IEEE Wireless Communications Letters*, vol. 2, no. 4, pp. 415–418, 2013.

[269] H. Xing, Y. Deng, K.-K. Wong, and A. Nallanathan, "Wireless powered large-scale multi-antenna af relaying for cooperative jamming-aided secrecy," in *International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*. IEEE, 2016, pp. 1–5.

[270] H. Xing, Z. Chu, Z. Ding, and A. Nallanathan, "Harvest-and-jam: Improving security for wireless energy harvesting cooperative networks," in *Global Communications Conference (GLOBECOM)*. IEEE, 2014, pp. 3145–3150.

[271] H. Xing, K.-K. Wong, Z. Chu, and A. Nallanathan, "To harvest and jam: A paradigm of self-sustaining friendly jammers for secure AF relaying," *IEEE transactions on signal processing*, vol. 63, no. 24, pp. 6616–6631, 2015.

[272] L. Xiao, T. Zhang, X. Shen, D. Yang, and L. Cuthbert, "Secrecy in Wireless Information and Power Transfer for One-Way and Two-Way Untrusted Relaying with Friendly Jamming," *Mobile Information Systems*, vol. 2017, 2017.

[273] H.-M. Wang, Q. Yin, W. Wang, and X.-G. Xia, "Joint null-space beamforming and jamming to secure af relay systems with individual power constraint," in *International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2013, pp. 2911–2914.

[274] Z. Ding, M. Peng, and H.-H. Chen, "A general relaying transmission protocol for MIMO secrecy communications," *IEEE Transactions on Communications*, vol. 60, no. 11, pp. 3461–3471, 2012.

[275] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Cooperative jamming for wireless physical layer security," in *Workshop on Statistical Signal Processing*. IEEE, 2009, pp. 417–420.

[276] S. S. Kalamkar and A. Banerjee, "Secure communication via a wireless energy harvesting untrusted relay," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 3, pp. 2199–2213, 2017.

[277] J. Moon, H. Lee, C. Song, and I. Lee, "Secrecy Performance Optimization for Wireless Powered Communication Networks With an Energy Harvesting Jammer," *IEEE Transactions on Communications*, vol. 65, no. 2, pp. 764–774, 2017.

[278] D. H. Ibrahim, E. S. Hassan, and S. A. El-Dolil, "A new relay and jammer selection schemes for secure one-way cooperative networks," *Wireless personal communications*, vol. 75, no. 1, pp. 665–685, 2014.
[279] N. T. Do, D. B. da Costa, T. Q. Duong, V. N. Q. Bao, and B. An, "Exploiting Direct Links in Multiuser Multirelay SWIPT Cooperative Networks With Opportunistic Scheduling," *IEEE Transactions on Wireless Communications*, vol. 16, no. 8, pp. 5410–5427, 2017.
[280] D. Wang, R. Zhang, X. Cheng, and L. Yang, "Capacity-Enhancing Full-Duplex Relay Networks based on Power-Splitting (PS-) SWIPT," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 6, pp. 5445–5450, 2017.
[281] F. Zhou, Z. Li, J. Cheng, Q. Li, and J. Si, "Robust AN-aided beamforming and power splitting design for secure MISO cognitive radio with SWIPT," *IEEE Transactions on Wireless Communications*, vol. 16, no. 4, pp. 2450–2464, 2017.
[282] Y. Dong, X. Ge, J. Hossain, J. Cheng, and V. C. Leung, "Proportional Fairness-Based Beamforming and Signal Splitting for MISO-SWIPT Systems," *IEEE Communications Letters*, vol. 21, no. 5, pp. 1135–1138, 2017.
[283] F. Jameel and S. Wyne, "Secrecy outage of SWIPT in the presence of cooperating eavesdroppers," *AEU-International Journal of Electronics and Communications*, vol. 77, pp. 23–26, 2017.
[284] F. Jameel, S. Wyne, S. J. Nawaz, J. Ahmed, and K. Cumanan, "On the Secrecy Performance of SWIPT Receiver Architectures with Multiple Eavesdroppers," *Wireless Communications and Mobile Computing (Hindawi)*, 2018.
[285] A. A. Nasir, H. D. Tuan, D. T. Ngo, T. Q. Duong, and H. V. Poor, "Beamforming design for wireless information and power transfer systems: Receive power-splitting versus transmit time-switching," *IEEE Transactions on Communications*, vol. 65, no. 2, pp. 876–889, 2017.
[286] S. Zhong, H. Huang, and R. Li, "Outage probability of power splitting swipt two-way relay networks in nakagami-m fading," *EURASIP Journal on Wireless Communications and Networking*, vol. 2018, no. 1, p. 11, 2018.
[287] Q. Shi, W. Xu, J. Wu, E. Song, and Y. Wang, "Secure beamforming for MIMO broadcasting with wireless information and power transfer," *IEEE Transactions on Wireless Communications*, vol. 14, no. 5, pp. 2841–2853, 2015.
[288] R. Feng, Q. Li, Q. Zhang, and J. Qin, "Robust secure transmission in MISO simultaneous wireless information and power transfer system," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 1, pp. 400–405, 2015.
[289] H. Xing, K.-K. Wong, and A. Nallanathan, "Secure wireless energy harvesting-enabled AF-relaying SWIPT networks," in *International Conference on Communications (ICC)*. IEEE, 2015, pp. 2307–2312.
[290] M. Tian, X. Huang, Q. Zhang, and J. Qin, "Robust AN-aided secure transmission scheme in MISO channels with simultaneous wireless information and power transfer," *IEEE Signal Processing Letters*, vol. 22, no. 6, pp. 723–727, 2015.
[291] L. Liu, R. Zhang, and K.-C. Chua, "Secrecy wireless information and power transfer with MISO beamforming," in *IEEE Global Communications Conference*. IEEE, 2013, pp. 1831–1836.
[292] Q. Zhang, X. Huang, Q. Li, and J. Qin, "Cooperative jamming aided robust secure transmission for wireless information and power transfer in MISO channels," *IEEE Transactions on Communications*, vol. 63, no. 3, pp. 906–915, 2015.
[293] Q. Li, Q. Zhang, and J. Qin, "Secure relay beamforming for simultaneous wireless information and power transfer in nonregenerative relay networks," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 5, pp. 2462–2467, 2014.
[294] X. Chen, J. Chen, and T. Liu, "Secure transmission in wireless powered massive MIMO relaying systems: Performance analysis and optimization," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 10, pp. 8025–8035, 2016.
[295] X. Chen, X. Wang, and X. Chen, "Energy-efficient optimization for wireless information and power transfer in large-scale MIMO systems employing energy beamforming," *IEEE Wireless Communications Letters*, vol. 2, no. 6, pp. 667–670, 2013.
[296] T. L. Marzetta, "Noncooperative cellular wireless with unlimited numbers of base station antennas," *IEEE Transactions on Wireless Communications*, vol. 9, no. 11, pp. 3590–3600, 2010.
[297] J. Zhu, R. Schober, and V. K. Bhargava, "Linear precoding of data and artificial noise in secure massive MIMO systems," *IEEE Transactions on Wireless Communications*, vol. 15, no. 3, pp. 2245–2261, 2016.
[298] Z. Jun, R. Schober, and V. K. Bhargava, "Secure transmission in multicell massive MIMO systems," *IEEE Transactions on Wireless Communications*, vol. 13, no. 9, pp. 4766–4781, 2014.
[299] J. Wang, J. Lee, F. Wang, and T. Q. Quek, "Jamming-aided secure communication in massive mimo rician channels," *IEEE Transactions on Wireless Communications*, vol. 14, no. 12, pp. 6854–6868, 2015.
[300] J. Vinogradova, E. Björnson, and E. G. Larsson, "Detection and mitigation of jamming attacks in massive MIMO systems using random matrix theory," in *17th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*. IEEE, 2016, pp. 1–5.
[301] T. Tai Do, E. Björnson, E. G. Larsson, and S. Mohammad Razavizadeh, "Jamming-resistant receivers for the massive mimo uplink," in *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 1. IEEE, 2018, pp. 210–223.
[302] J. Vinogradova, E. Björnson, and E. G. Larsson, "Jamming massive MIMO using massive MIMO: Asymptotic separability results," in *International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2017, pp. 3454–3458.
[303] S. Mumtaz, A. Alsohaily, Z. Pang, A. Rayes, K. F. Tsang, and J. Rodriguez, "Massive Internet of Things for Industrial Applications: Addressing Wireless IIoT Connectivity Challenges and Ecosystem Fragmentation," *IEEE Industrial Electronics Magazine*, vol. 11, no. 1, pp. 28–33, 2017.
[304] R. Fantacci, T. Pecorella, R. Viti, and C. Carlini, "Short paper: Overcoming IoT fragmentation through standard gateway architecture," in *World Forum on Internet of Things (WF-IoT)*. IEEE, 2014, pp. 181–182.
[305] F. Romano, T. Pecorella, R. Viti, and C. Carlini, "A network architecture solution for efficient IoT WSN backhauling: challenges and opportunities," *IEEE Wireless Communications*, vol. 21, no. 4, pp. 113–119, 2014.
[306] A. Mukherjee, "Physical-layer security in the internet of things: Sensing and communication confidentiality under resource constraints," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1747–1761, 2015.
[307] F. Jameel, M. A. Javed, D. N. Jayakody, and S. A. Hassan, "On secrecy performance of industrial Internet of things," *Internet Technology Letters*, vol. 1, no. 2, p. e32, 2018.
[308] T. Pecorella, L. Brilli, and L. Mucchi, "The Role of Physical Layer Security in IoT: A Novel Perspective," *Information*, vol. 7, no. 3, p. 49, 2016.
[309] S. Vuppala, Y. J. Tolossa, G. Kaddoum, and G. Abreu, "On the physical layer security analysis of hybrid millimeter wave networks," *IEEE Transactions on Communications*, vol. 66, no. 3, pp. 1139–1152, 2018.
[310] Y. Zhu, L. Wang, K.-K. Wong, and R. W. Heath, "Secure communications in millimeter wave ad hoc networks," *IEEE Transactions on Wireless Communications*, vol. 16, no. 5, pp. 3205–3217, 2017.
[311] S. Gong, C. Xing, Z. Fei, and S. Ma, "Millimeter-wave secrecy beamforming designs for two-way amplify-and-forward MIMO relaying networks," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 3, pp. 2059–2071, 2017.
[312] S. Gong, C. Xing, Z. Fei, and J. Kuang, "Secrecy beamforming design for large millimeter-wave two-way relaying networks," in *Wireless Communications and Networking Conference (WCNC)*. IEEE, 2016, pp. 1–6.
[313] Y. Zhu, L. Wang, K.-K. Wong, and R. W. Heath, "Physical layer security in large-scale millimeter wave ad hoc networks," in *Global Communications Conference (GLOBECOM)*. IEEE, 2016, pp. 1–6.
[314] Y. R. Ramadan, A. S. Ibrahim, and M. M. Khairy, "RF beamforming for secrecy millimeter wave MISO-OFDM systems," in *International Conference on Communications (ICC)*. IEEE, 2016, pp. 1–6.
[315] F. Boccardi, R. W. Heath, A. Lozano, T. L. Marzetta, and P. Popovski, "Five disruptive technology directions for 5G," *IEEE Communications Magazine*, vol. 52, no. 2, pp. 74–80, 2014.
[316] Y. Wang, J. Li, L. Huang, Y. Jing, A. Georgakopoulos, and P. Demestichas, "5G mobile: Spectrum broadening to higher-frequency bands to support high data rates," *IEEE Vehicular technology magazine*, vol. 9, no. 3, pp. 39–46, 2014.
[317] M. J. Saber and S. M. S. Sadough, "On secure free-space optical communications over málaga turbulence channels," *IEEE Wireless Communications Letters*, vol. 6, no. 2, pp. 274–277, 2017.
[318] A. Asadi and V. Mancuso, "Network-assisted Outband D2D-clustering in 5G Cellular Networks: Theory and Practice," *IEEE Transactions on Mobile Computing*, vol. 16, no. 8, pp. 2246–2259, 2017.
[319] A. Zhang and X. Lin, "Security-Aware and Privacy-Preserving D2D Communications in 5G," *IEEE Network*, vol. 31, no. 4, pp. 70–77, 2017.
[320] F. Jameel, Z. Hamid, F. Jabeen, S. Zeadally, and M. A. Javed, "A Survey of Device-to-Device Communications: Research Issues and Challenges," *IEEE Communications Surveys Tutorials*, pp. 1–1, 2018.

[321] K. Zhang, M. Peng, P. Zhang, and X. Li, "Secrecy-optimized resource allocation for device-to-device communication underlaying heterogeneous networks," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 2, pp. 1822–1834, 2017.

[322] F. Alavi, N. M. YAMCHI, M. R. Javan, and K. Cumanan, "Limited Feedback Scheme for Device to Device Communications in 5G cellular networks with Reliability and Cellular Secrecy Outage Constraints," *IEEE Transactions on Vehicular Technology*, 2017.

[323] S. Vuppala and G. Kaddoum, "Secrecy capacity analysis in D2D underlay cellular networks: Colluding eavesdroppers," in *Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*. IEEE, 2017, pp. 1–7.

[324] J. Yue, C. Ma, H. Yu, and W. Zhou, "Secrecy-based access control for device-to-device communication underlaying cellular networks," *IEEE Communications Letters*, vol. 17, no. 11, pp. 2068–2071, 2013.

[325] C. Ma, J. Liu, X. Tian, H. Yu, Y. Cui, and X. Wang, "Interference exploitation in D2D-enabled cellular networks: A secrecy perspective," *IEEE Transactions on Communications*, vol. 63, no. 1, pp. 229–242, 2015.

[326] Z. Chu, K. Cumanan, M. Xu, and Z. Ding, "Robust secrecy rate optimisations for multiuser multiple-input-single-output channel with device-to-device communications," *IET Communications*, vol. 9, no. 3, pp. 396–403, 2014.

[327] F. Jameel, F. Khan, M. A. A. Haider, and A. U. Haq, "Secrecy analysis of relay assisted device-to-device systems under channel uncertainty," in *International Conference on Frontiers of Information Technology (FIT)*, vol. 1, no. 1, Dec 2017, pp. 345–349.

[328] Y. Saito, Y. Kishiyama, A. Benjebbour, T. Nakamura, A. Li, and K. Higuchi, "Non-orthogonal multiple access (NOMA) for cellular future radio access," in *Vehicular Technology Conference (VTC Spring), 2013 IEEE 77th*. IEEE, 2013, pp. 1–5.

[329] C. Zhong and Z. Zhang, "Non-orthogonal multiple access with cooperative full-duplex relaying," *IEEE Communications Letters*, vol. 20, no. 12, pp. 2478–2481, 2016.

[330] Z. Ding, M. Peng, and H. V. Poor, "Cooperative non-orthogonal multiple access in 5G systems," *IEEE Communications Letters*, vol. 19, no. 8, pp. 1462–1465, 2015.

[331] S. Lee, D. B. Da Costa, Q.-T. Vien, T. Q. Duong, and R. T. de Sousa Jr, "Non-orthogonal multiple access schemes with partial relay selection," *IET Communications*, vol. 11, no. 6, pp. 846–854, 2016.

[332] Z. Ding, H. Dai, and H. V. Poor, "Relay selection for cooperative NOMA," *IEEE Wireless Communications Letters*, vol. 5, no. 4, pp. 416–419, 2016.

[333] J. Men and J. Ge, "Non-orthogonal multiple access for multiple-antenna relaying networks," *IEEE Communications Letters*, vol. 19, no. 10, pp. 1686–1689, 2015.

[334] X. Yue, Y. Liu, S. Kang, and A. Nallanathan, "Performance Analysis of NOMA With Fixed Gain Relaying Over Nakagami-m Fading Channels," *IEEE Access*, vol. 5, pp. 5445–5454, 2017.

[335] J. Men, J. Ge, and C. Zhang, "Performance Analysis for Downlink Relaying Aided Non-Orthogonal Multiple Access Networks With Imperfect CSI Over Nakagami-m Fading," *IEEE Access*, vol. 5, pp. 998–1004, 2017.

[336] M. Jinjin, J. Ge, and C. Zhang, "Performance Analysis of Nonorthogonal Multiple Access for Relaying Networks Over Nakagami-m Fading Channels," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 2, pp. 1200–1208, 2017.

[337] Z. Qin, Y. Liu, Z. Ding, Y. Gao, and M. Elkashlan, "Physical layer security for 5G non-orthogonal multiple access in large-scale networks," in *Communications (ICC), 2016 IEEE International Conference on*. IEEE, 2016, pp. 1–6.

[338] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, and L. Hanzo, "Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks," *IEEE Transactions on Wireless Communications*, vol. 16, no. 3, pp. 1656–1672, 2017.

[339] B. Zheng, M. Wen, C.-X. Wang, X. Wang, F. Chen, J. Tang, and F. Ji, "Secure NOMA Based Two-Way Relay Networks Using Artificial Noise and Full Duplex," *IEEE Journal on Selected Areas in Communications*, 2018.

[340] J. Chen, L. Yang, and M.-S. Alouini, "Physical layer security for cooperative NOMA systems," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 5, pp. 4645–4649, 2018.

[341] G. I. Tsiropoulos, O. A. Dobre, M. H. Ahmed, and K. E. Baddour, "Radio resource allocation techniques for efficient spectrum access in cognitive radio networks," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 824–847, 2016.

[342] H. Reyes, S. Subramaniam, N. Kaabouch, and W. C. Hu, "A spectrum sensing technique based on autocorrelation and Euclidean distance and its comparison with energy detection for cognitive radio networks," *Computers & Electrical Engineering*, vol. 52, pp. 319–327, 2016.

[343] N. Zhao, F. R. Yu, H. Sun, and M. Li, "Adaptive power allocation schemes for spectrum sharing in interference-alignment-based cognitive radio networks," *IEEE transactions on vehicular technology*, vol. 65, no. 5, pp. 3700–3714, 2016.

[344] T. Jiang, T. Li, and J. Ren, "Toward secure cognitive communications in wireless networks," *IEEE Wireless Communications*, vol. 19, no. 4, 2012.

[345] H. Lei, H. Zhang, I. S. Ansari, C. Gao, Y. Guo, G. Pan, and K. A. Qaraqe, "Secrecy outage performance for SIMO underlay cognitive radio systems with generalized selection combining over Nakagami-m channels," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 12, pp. 10 126–10 132, 2016.

[346] G. Rathee, P. Thakur, G. Singh, and H. Saini, "Aspects of secure communication during spectrum handoff in cognitive radio networks," in *International Conference on Signal Processing and Communication (ICSC)*. IEEE, 2016, pp. 64–69.

[347] A. G. Fragkiadakis, E. Z. Tragos, and I. G. Askoxylakis, "A survey on security threats and detection techniques in cognitive radio networks," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 1, pp. 428–445, 2013.

[348] L. Jianwu, F. Zebing, F. Zhiyong, and Z. Ping, "A survey of security issues in cognitive radio networks," *China Communications*, vol. 12, no. 3, pp. 132–150, 2015.

[349] Y. Pei, Y.-C. Liang, L. Zhang, K. C. Teh, and K. H. Li, "Secure communication over MISO cognitive radio channels," *IEEE Transactions on Wireless Communications*, vol. 9, no. 4, pp. 00–00, 2010.

[350] P. Maji, B. Prasad, S. D. Roy, and S. Kundu, "Secrecy Outage of a Cognitive Radio Network with Selection of Energy Harvesting Relay and Imperfect CSI," *Wireless Personal Communications*, pp. 1–16.

[351] D. W. K. Ng, E. S. Lo, and R. Schober, "Multiobjective resource allocation for secure communication in cognitive radio networks with wireless information and power transfer," *IEEE transactions on vehicular technology*, vol. 65, no. 5, pp. 3166–3184, 2016.

[352] W. Li, M. Xin, M. Yue, T. Yinglei, and Z. Yong, "Security-oriented transmission based on cooperative relays in cognitive radio," *China Communications*, vol. 10, no. 8, pp. 27–35, 2013.

[353] Y. Wu and X. Chen, "Robust beamforming and power splitting for secrecy wireless information and power transfer in cognitive relay networks," *IEEE Communications Letters*, vol. 20, no. 6, pp. 1152–1155, 2016.

[354] Y. Liu, L. Wang, T. T. Duy, M. Elkashlan, and T. Q. Duong, "Relay selection for security enhancement in cognitive relay networks," *IEEE Wireless Communications Letters*, vol. 4, no. 1, pp. 46–49, 2015.

[355] Y. Zou, B. Champagne, W.-P. Zhu, and L. Hanzo, "Relay-selection improves the security-reliability trade-off in cognitive radio systems," *IEEE Transactions on Communications*, vol. 63, no. 1, pp. 215–228, 2015.

[356] G. Tuna, D. G. Kogias, V. C. Gungor, C. Gezer, E. Taşkın, and E. Ayday, "A survey on information security threats and solutions for Machine to Machine (M2M) communications," *Journal of Parallel and Distributed Computing*, vol. 109, pp. 142–154, 2017.

[357] P. H. Nardelli, H. Alves, C. H. De Lima, and M. Latva-Aho, "Throughput maximization in multi-hop wireless networks under a secrecy constraint," *Computer Networks*, vol. 109, pp. 13–20, 2016.